Guides pratiques

Chaque Guide pratique explique comment utiliser un gratuiciel ou un logiciel de source ouverte (Open Source). On y présente les difficultés potentielles, on y donne des conseils pratiques et, surtout, on vous montre comment configurer et utiliser ces outils de façon sûre. Chaque guide comporte plusieurs captures d'écran, ainsi qu'un mode d'emploi point par point pour vous aider à suivre la démarche.

Tous ces logiciels peuvent être installés directement à partir du Guide pratique ou téléchargés gratuitement du site du développeur. Dans la plupart des cas, il vous sera possible d'installer un outil simplement en cliquant sur le lien approprié situé au début du guide associé à cet outil, puis en indiquant à votre navigateur d'Ouvrir ou d'Installer le programme. Si un Guide pratique fournit des instructions d'installation particulières, il vous faudra peut-être sauvegarder un fichier sur votre Bureau ou à un autre emplacement avant d'installer cet outil.

La trousse à outils Security in-a-box comprend également une section appelée Sécurité portable, où vous trouverez des versions « portables » de certains outils importants. Ces versions sont conçues pour être installées directement sur une clé USB pour que vous puissiez les utiliser à partir de n'importe quel ordinateur.

Pour des raisons de sécurité, vous devriez toujours utiliser la plus récente version des programmes présentés ici. La version de certains des programmes présentés ici est peut-être plus récente que celle utilisée pour rédiger le guide pratique correspondant. Dans ce cas, l'interface de la nouvelle version peut différer légèrement de celle décrite dans ce guide, mais pas substantiellement.

Avast - antivirus

Short Description:

avast! est un programme antivirus complet qui sert à détecter et éliminer les virus et logiciels malveillants de votre ordinateur. Bien qu'**avast!** soit gratuit pour utilisation non commerciale sur un ordinateur familial ou personnel, votre copie gratuite *doit* être enregistrée après l'installation, à défaut de quoi elle expirera après 30 jours. L'enregistrement vous assurera également de recevoir automatiquement les mises à jour du programme **Avast!**, ainsi que les plus récentes définitions de virus au fur et à mesure de leur publication.

Online Installation Instructions:

Pour installer avast!

- *Lisez la courte **Introduction** aux **Guides pratiques** [1]*
- ***Cliquez** sur l'icone **avast!** ci-dessous pour ouvrir la page de téléchargement d'**www.avast.com**.*
- ***Cliquez** sur le bouton 'Télécharger' au bas de la colonne 'Antivirus Gratuit', puis **cliquez** sur le lien 'Télécharger' qui s'affiche sur la prochaine page.*
- ***Cliquez** sur 'Enregistrer le fichier' pour sauvegarder le fichier 'setup_av_free_fre.exe' sur votre ordinateur, puis **double-cliquez** sur 'setup_av_free_fre.exe' pour lancer l'installation du programme.*
- *Lisez attentivement la section **2.0 Comment installer et enregistrer avast!** avant de poursuivre.*
- *Après avoir complété l'installation d'**avast!** vous pouvez supprimer l'exécutable d'installation de votre ordinateur.*

avast!:

[2]

Site Internet:

www.avast.com [3]

Configuration requise:

- Compatible avec toutes les versions de Windows

Version utilisée pour rédiger ce guide:

- 5.0

Licence:

- Gratuiciel

Lecture préalable:

- **Livret pratique** Security-in-a-Box, chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** [4]

Niveau: 1: Débutant, **2: Moyen**, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 20 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de scanner votre ordinateur pour y détecter des virus et les éliminer.
- La capacité de protéger votre ordinateur contre les nouveaux virus et toute nouvelle infection.

- La capacité de recevoir des mises à jour des définitions de virus depuis Internet.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Bien que nous recommandions l'**antivirus gratuit d'avast!** dans ce chapitre, il existe d'autres programmes compatibles avec **Microsoft Windows** qui valent également la peine qu'on s'y intéresse:

- **Avira AntiVir Personal Edition** [5] et
- **AVG Anti-Virus** [6].

Par ailleurs, si vous avez les moyens d'acheter la version commerciale du programme antivirus pour **Microsoft Windows**, vous en retirerez probablement une protection plus complète.

Bien que les systèmes d'exploitation comme **GNU Linux** et **Mac OS** soient pratiquement épargnés des virus, il existe plusieurs bonnes raisons pour y installer des programmes contre les virus et les programmes malveillants. D'abord, des virus seront éventuellement créés pour ces systèmes d'exploitation, et deuxièmement, vous courez le risque de répandre des virus à votre insu, même si votre propre système est protégé.

À l'heure actuelle, il n'existe malheureusement aucun programme antivirus *gratuit* que nous serions à l'aise de recommander pour **Linux** et **Mac OS**. Cependant, il existe plusieurs produits *commerciaux* qui présentent de nombreux avantages et une excellente protection. Voici la liste des programmes les plus populaires:

- **avast!** [7],
- **Kaspersky** [8],
- **Mcafee** [9],
- **Sophos** [10], et
- **Symantec** [11], entre autres.

Si vous pouvez vous permettre d'acheter une copie de l'un ou l'autre de ces programmes, n'hésitez pas à le faire.

1.1 À propos de cet outil

Les virus informatiques sont des programmes malveillants qui peuvent détruire des fichiers, ralentir votre ordinateur et utiliser votre carnet d'adresses pour trouver et infecter d'autres ordinateurs. Avast est un programme antivirus complet qui protège votre ordinateur contre les virus qui pourraient y accéder par téléchargement depuis Internet, par courriel (pièce jointe) ou par transfert depuis un support amovible (CD, DVD, disquette, clé USB, etc.).

- Assurez-vous de ne pas avoir deux programmes antivirus installés et actifs simultanément. Si vous utilisez présentement un autre programme et souhaitez changer pour **avast!**, vous devez d'abord désinstaller l'autre programme antivirus avant d'installer **avast!**.

- De nouveaux virus sont conçus à tous les jours. Pour protéger efficacement votre ordinateur, **avast!** doit être en mesure de mettre à jour régulièrement votre base de données virale.

- Les virus les plus insidieux sont ceux qui empêchent carrément l'installation d'**avast!** et ceux qu'**avast!** n'est pas en mesure de détecter et supprimer. Dans une situation comme celle-là, il vous faudra recourir à des méthodes un peu plus avancées, dont certaines sont abordées à la section **4.9 Méthodes avancées de suppression des virus** [12].

Offline Installation Instructions :

Pour installer avast!

- *Lisez la courte **Introduction** aux **Guides pratiques** [13]**
- ***Cliquez sur l'icone avast! ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.*
- *Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

avast!:

[14]

Comment installer et enregistrer avast!

Sommaire des sections de cette page:

- **2.0 Comment installer avast!**
- **2.1 Comment enregistrer avast!**

2.0 Comment installer avast!

L'installation d'**avast!** est relativement simple et rapide. Pour commencer, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** sur setup_av_free_fre ; si une fenêtre *Fichier ouvert - Avertissement de sécurité* s'affiche, **cliquez** sur Exécuter pour activer la barre de progression du décompactage, qui peut prendre jusqu'à une minute, selon la vitesse de votre ordinateur. Lorsque toutes les composantes d'**avast!** seront décompactées, la boîte de dialogue suivante s'affichera (NDT: Si vous installez le programme à partir du fichier d'installation français, l'assistant passe directement à la deuxième étape décrite ci-dessous.)

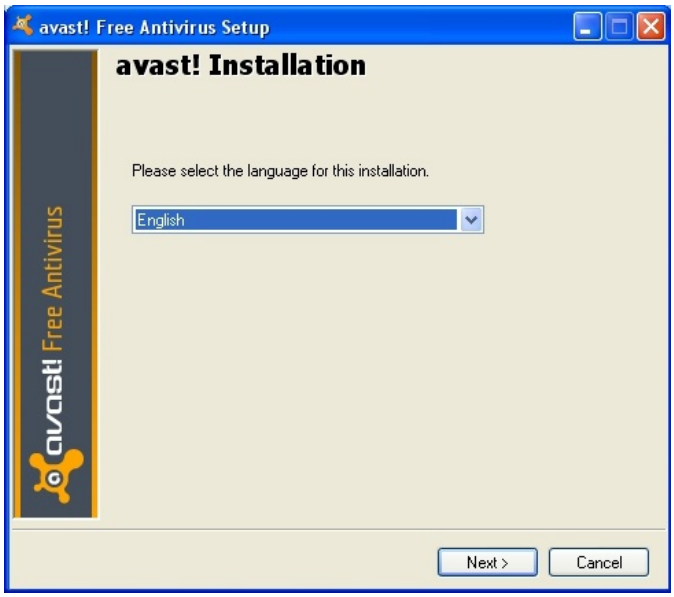


Figure 1: La fenêtre d'installation d'avast! Free Antivirus

Deuxième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

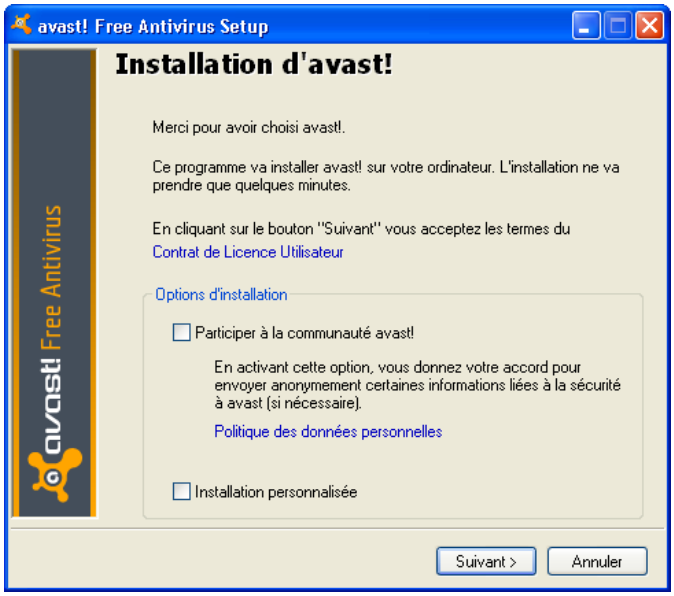

avast! Free Antivirus Setup
Installation d'avast!
Merci pour avoir choisi avast!.
Ce programme va installer avast! sur votre ordinateur. L'installation ne va prendre que quelques minutes.
En cliquant sur le bouton "Suivant" vous acceptez les termes du
Contrat de Licence Utilisateur
Options d'installation
Participer à la communauté avast!
En activant cette option, vous donnez votre accord pour envoyer anonymement certaines informations liées à la sécurité à avast (si nécessaire).
Politique des données personnelles
Installation personnalisée
avast! Free Antivirus
Suivant >
Annuler

Figure 2: La fenêtre d'installation d'avast!

Lors du processus d'installation d'**avast!*, la fenêtre d'installation s'affiche avec l'option *Participer à la communauté avast!* automatiquement sélectionnée. Pour des raisons de sécurité et de confidentialité, il est préférable que vous désactiviez cette option, tel qu'illustré à la *Figure 2*, ci-dessus.

Troisième étape. **Décochez** la case *Participer à la communauté avast!* pour dessélectionner cette option, puis **cliquez** sur Suivant > pour afficher la prochaine fenêtre:

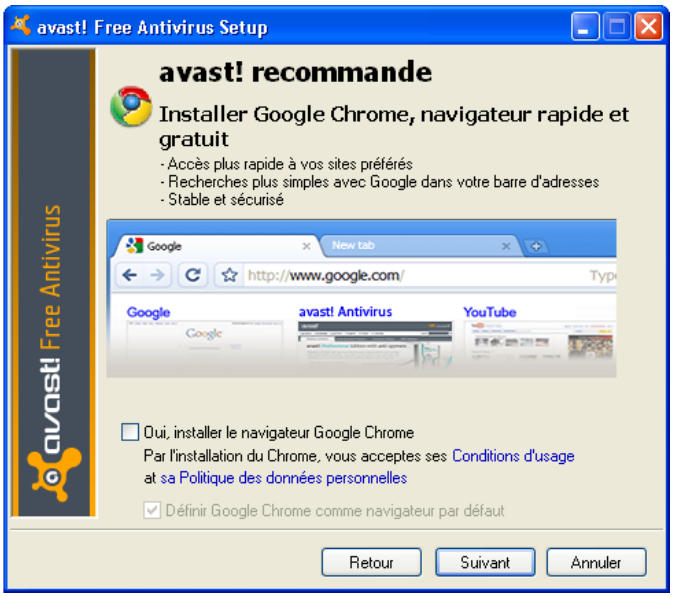


Figure 3: La fenêtre avast! recommande

Lors du processus d'installation d'**avast!**, la fenêtre *avast! recommande* s'affiche avec l'option *Oui, installer le navigateur Google Chrome* automatiquement sélectionnée. Il est préférable de désactiver cette option, tel qu'illustré à la figure 3, ci-dessus.

Quatrième étape. **Décochez** la case *Oui, installer le navigateur Google Chrome* pour dessélectionner cette option, puis **cliquez** sur Suivant > pour poursuivre l'installation d'**avast!**.

Un message s'affichera après quelques minutes pour vous indiquer que le processus d'installation est terminé.

Cinquième étape. **Cliquez** sur Fin pour finaliser le processus d'installation du logiciel. Quelques secondes plus tard, un icone **avast!** apparaît dans votre *Barre d'état système*:

Figure 4: L'icone avast! surlignée en noir dans Barre d'état système

Quelques secondes plus tard, un autre message s'affiche pour confirmer l'installation d'**avast!**:

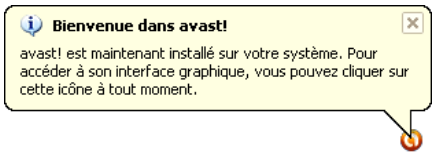

Bienvenue dans avast!
avast! est maintenant installé sur votre système. Pour accéder à son interface graphique, vous pouvez cliquer sur cette icône à tout moment.

Figure 5: Le message de confirmation de l'installation d'avast!

Chaque fois qu'**avast!** opère une mise à jour automatique du programme ou de la base de données virale, un message s'affiche au dessus de la *Barre d'état système*, tel qu'illustré ci-dessous:

Figure 6: Un exemple de message d'avast!

Important: Vous *devez* enregistrer votre copie du programme pour vous assurer que la base de données virale et le logiciel lui-même soient régulièrement mis à jour automatiquement.

Lorsque vous aurez correctement enregistré votre copie d'**avast!**, le programme protégera automatiquement votre ordinateur contre les virus et les logiciels malveillants. En cas d'attaque, **avast!** affichera des messages d'avertissement comme celui-ci:

LOGICIEL MALVEILLANT BLOQUÉ
Le Agent Web avast! a bloqué une menace.
Aucune autre action n'est demandée.
Objet : ...://www.securite-informatique.info/virus/eicar/download/eicar.zip|>eica
Infection : EICAR Test-NOT virus!!!
Action : Connexion interrompue
Processus : C:\Program Files\Mozilla Firefox\firefox.exe
La menace a été détectée et bloquée pendant le téléchargement.
Plus d'informations
avast!

Figure 7: Un exemple d'avertissement indiquant qu'une menace a été bloquée.

Sixième étape. **Double-cliquez** sur dans la *Barre d'état système* (voir la figure 4) pour ouvrir la fenêtre principale d'**avast!**, puis **cliquez** sur Plus de détails... pour afficher les détails de l'*État actuel*, tel qu'illustré ci-dessous:

Figure 8: La fenêtre principale du programme avast!

Important: Vous devez enregistrer **avast!** pour continuer à recevoir les mises à jour du programme et des définitions de virus, qui sont essentielles à la protection de votre ordinateur contre diverses menaces.

2.1 Comment enregistrer avast!

Commentaire: Si vous n'enregistrez pas votre copie d'**avast!**, celle-ci cessera de fonctionner après 30 jours. Il vous faut être connecté à Internet pour enregistrer **avast!**.

Pour enregistrer votre copie d'**avast!**, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur pour afficher la fenêtre principale d'**avast!** (*Figure 10*).

Deuxième étape. **Cliquez** sur Enregistrez-vous maintenant (par les menus MAINTENANCE et Enregistrement) pour afficher les deux fenêtres suivantes successivement:

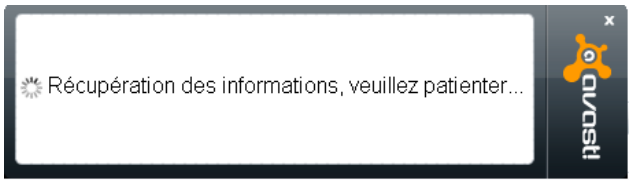


Figure 9: Fenêtre d'enregistrement d'avast! antivirus gratuit

La fenêtre d'*Enregistrement d'avast! antivirus gratuit* vous informe que des informations sont en cours de récupération. Une deuxième fenêtre vous avise que votre copie d'**avast!** expirera dans 30 jours si vous ne l'enregistrez pas d'ici là. (La même fenêtre affiche également des renseignements sur les versions commerciales du logiciel et les promotions en cours.)

Votre protection avast! expirera dans 30 jours
Mettez votre protection à niveau maintenant et économisez 50%
-50%
Continuer à utiliser avast! Antivirus Gratuit
Mise à niveau vers avast! Internet Security
Antivirus et anti-espion
Navigation sécurisée (avast! Sandbox)
Pare-feu contre les attaques de pirates
Filtrage contre le spam et le hameçonnage
Quel est le produit le plus adapté ?
Pour une utilisation classique d'Internet, enregistrez-vous avast! Antivirus Gratuit
Si vous effectuez des achats ou des activités bancaires en ligne, procédez à une mise à avast! Internet Security
S'enregistrer
Ai-je besoin d'une protection supplémentaire ?
C$ 69.95 C$ 34.98
Mettez à niveau
Effectuez une mise à niveau 2 ans et économisez C$ 67
Autres options
Je possède déjà une licence
Me le rappeler ultérieurement

Figure 10: La fenêtre d'état de votre enregistrement

Troisième étape. **Cliquez** sur pour afficher à nouveau la boîte illustrée à la *figure 2*, suivie immédiatement de cette fenêtre:

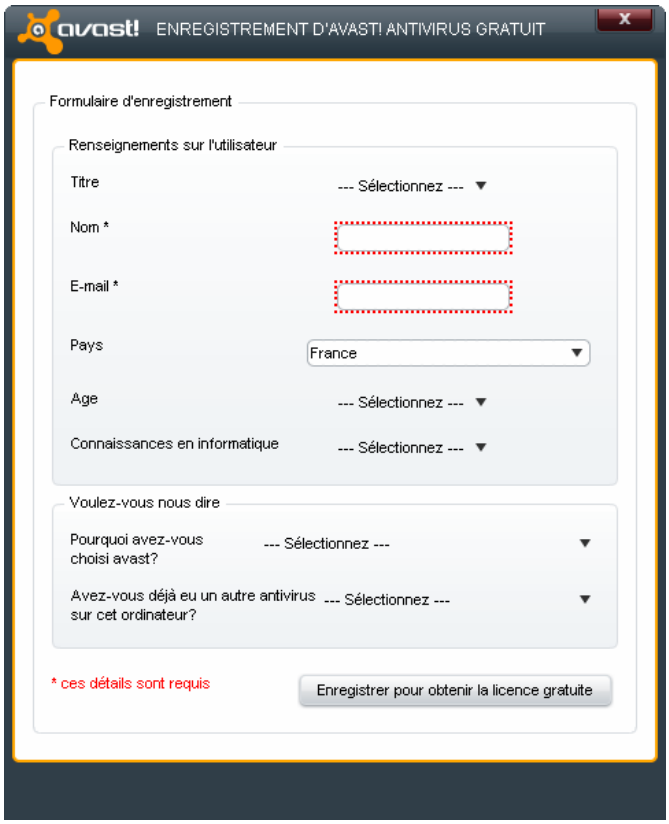
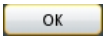


Figure 11: Le formulaire d'enregistrement d'avast! antivirus gratuit

Commentaire: Les seuls champs *obligatoires* sont le *Nom* et l'*E-mail*. Ils sont identifiés par des astérisques et encadrés d'une ligne pointillée rouge. Les autres champs sont facultatifs.

Quatrième étape. **Saisissez** votre nom et votre adresse de courriel dans les champs appropriés, puis **cliquez** sur pour afficher la prochaine fenêtre:

Figure 12: Fenêtre pop-up Merci pour votre enregistrement

Cinquième étape. **Cliquez** sur  pour afficher le panneau *VOTRE ENREGISTREMENT* dans la fenêtre principale du

programme:

avast! ANTIVIRUS GRATUIT
CENTRE D'AIDE
PARAMÈTRES
METTRE À NIVEAU
RÉSUMÉ
LANCER UN SCAN
PROTECTION RÉSIDENTE
MAINTENANCE
Mise à jour
Enregistrement
Zone de Quarantaine
A propos d'avast!
VOTRE ENREGISTREMENT
Vous pouvez vérifier les détails concernant votre enregistrement de avast! Free Antivirus.
ETAT ACTUEL : ENREGISTRÉ
Informations sur l'enregistrement
Votre enregistrement va expirer le : 2011-08-17 18:14:21
Date d'enregistrement : 2010-08-17 18:14:21
Mettre à niveau
Si vous avez acheté une mise à niveau vers avast! Antivirus Pro ou avast! Internet Security, veuillez saisir le fichier de licence reçu en cliquant sur ce bouton.
Saisir le fichier de licence avast! Antivirus Pro / avast! Internet Security

Figure 13: Le panneau VOTRE ENREGISTREMENT qui confirme l'enregistrement de votre copie d'avast!

Vous avez complété l'enregistrement de votre copie d'**avast!** et êtes maintenant en position d'apprendre comment mettre manuellement à jour le programme et les définitions de virus. Pour ce faire, veuillez lire la section **3.0 Comment mettre à jour avast! manuellement**.

Comment mettre à jour avast! manuellement

Sommaire des sections de cette page :

- **3.0 Avant de commencer**
- **3.1 Comment lancer une mise à jour par l'interface principale d'avast!**
- **3.2 Comment lancer une mise à jour par le menu local d'avast!**
- **3.3 Comment désactiver la fonction de mise à jour automatique d'avast!**

3.0 Avant de commencer

avast! marche discrètement en arrière-plan de votre ordinateur et exécute automatiquement des mises à jour du programme et des définitions de virus chaque fois que vous vous connectez à Internet. Cela dit, si votre accès à Internet est temporaire ou sporadique, il sera peut-être plus pratique ou efficace de lancer les mises à jour manuellement lorsque cela vous convient.

Commentaire: Il existe deux méthodes pour lancer les mises à jour d'**avast!** manuellement. Vous pouvez lancer une mise à jour à partir de l'interface principale d'**avast!** ou en passant par le menu local qui se déploie lorsque vous cliquez à droite sur l'icone **avast!** de la *Barre d'état système*. De plus, il est possible de désactiver l'option de mise à jour automatique dans la fenêtre *RÉGLAGES PRINCIPAUX*, en **cliquant** sur dans le coin supérieur droit de l'interface principale.

Comment lancer une mise à jour par l'interface principale d'avast!

Pour mettre à jour **avast!** manuellement à partir de l'interface principale, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur pour afficher l'interface principale d'**avast!**, illustrée ci-dessous:

Figure 1: L'onglet Résumé affichant le panneau État actuel, où figure un avis typique de mise à jour de la Version du programme

Une mise à jour du programme ou des définitions de virus est indiquée par un icone orange marqué d'un point d'exclamation, au lieu de l'icone vert marqué d'un crochet. La mise à jour du programme ou de la définition de virus est affichée en rouge et un bouton *Mise à jour* est désormais visible.

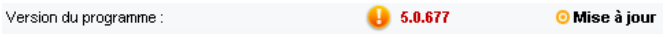


Figure 2: Une nouvelle version du programme est disponible

Deuxième étape: **Cliquez** sur pour lancer la mise à jour. À l'issue de la mise à jour, la sous-fenêtre *Version du programme* s'affiche comme ceci:

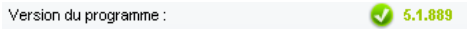


Figure 3: La Version du programme est mise à jour

Le programme est passé de la version 5.0.677 à la version 5.1.889.

La liste ci-dessous décrit brièvement chacun des items ou icones d'état du panneau *État actuel SÉCURISÉ*:

Astuce: **Cliquez** sur pour afficher ou cacher les renseignements du panneau *État actuel*

Protection résidente: Cet icone indique si la protection résidente fonctionne normalement. La protection résidente surveille l'activité de votre ordinateur; il y a des protections résidentes dédiées au courriel, au système de fichier local, à l'activité sur Internet, ainsi qu'à d'autre systèmes. Lorsqu'une protection résidente est désactivée, que ce soit volontairement ou sous l'effet d'un programme malveillant, l'icone d'**avast** dans la *Barre d'état système* change d'apparence pour refléter ce changement d'état:

Mise à jour automatique de la VPS: Cet icone indique si le mécanisme de mise à jour automatique est activé ou non.

Version de la base de données virale VPS: Cet icone indique la date de publication de la plus récente définition de virus. La date est affichée de la façon suivante: 11 réfère à l'année 2011, 01 réfère au mois et 17 réfère au jour.

Version du programme: Cet icone indique la plus récente mise à jour de la version du programme.

Date d'expiration: Cet item indique la date et l'heure d'expiration de votre copie d'**avast!**; vous devez renouveler ou ré-enregistrer votre copie avant cette date.

Troisième étape. **Cliquez** sur pour afficher la fenêtre ci-dessous:

avast! ANTIVIRUS GRATUIT
CENTRE D'AIDE
PARAMÈTRES
METTRE À NIVEAU
RÉSUMÉ
LANCER UN SCAN
PROTECTION RÉSIDENTE
MAINTENANCE
Mise à jour
Enregistrement
Zone de Quarantaine
A propos d'avast!
MISE À JOUR
Il est très important de maintenir votre logiciel de sécurité à jour. avast! est conçu pour se mettre à jour automatiquement, vous pouvez cependant gérer les mises à jour manuellement.
Mettre à jour le moteur et la base de données virale VPS
Version actuelle : 110117-1
Date de publication : 2011-01-17 13:09:03
Nombre de définitions : 2 409 316
La quantité réelle de logiciels malveillants qu'avast! peut détecter est bien supérieure à ce nombre parce qu'une définition peut identifier des dizaines, centaines ou parfois même des milliers de logiciels malveillants distincts.
Dernier essai de mise à jour il y a : 6 minutes
Mettre à jour le programme
Version actuelle : 5.1.889

Figure 4: L'interface principale affichant le panneau MAINTENANCE MISE À JOUR

Le panneau *MAINTENANCE MISE À JOUR* peut être utilisé pour mettre à jour manuellement le programe et les définitions de virus.

Quatrième étape: **Cliquez** sur

pour lancer la mise à jour du moteur et des définitions de virus.

Cinquième étape: **Cliquez** sur

quand la mise à jour est complétée pour retourner au panneau *MAINTENANCE MISE À JOUR*.

Le processus est le même pour mettre à jour le programme **avast!**.

Sixième étape: **Cliquez** sur

pour lancer la mise à jour du programme.

Septième étape: **Cliquez** sur

quand la mise à jour est complétée pour retourner au panneau *MAINTENANCE MISE À JOUR*.

3.2 Comment lancer une mise à jour par le menu local d'avast!

Les mises à jour du programme et des définitions de virus d'**avast!** peuvent être exécutées à partir du menu local **avast!**. Il est possible d'accéder directement au panneau *MAINTENANCE MISE À JOUR* d'**avast!** par le menu local qui se trouve dans la *Barre d'état système*.

Pour lancer manuellement les mises à jour du *moteur et de la base de données virale* à partir du menu local, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez à droite** sur dans la *barre d'état système* pour afficher le menu local illustré ci-dessous:

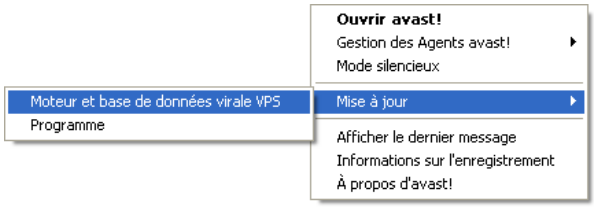


Figure 5: Le menu local d'avast!

Deuxième étape: **Sélectionnez Mise à jour > Moteur et base de données virale VPS** pour afficher la *Figure 4*, puis suivez les **étapes 4 et 5**.

Troisième étape: **Sélectionnez Mise à jour > Programme** pour afficher la *Figure 6*, puis suivez les *étapes 6 et 7* décrite à la section **3.1 Comment lancer une mise à jour par l'interface principale d'avast!**

3.3 Comment désactiver la fonction de mise à jour automatique d'avast!

En mode par défaut, **avast!** est configuré pour télécharger automatiquement les mises à jour du programme et de la base de données virale. Vous pouvez cependant désactiver cette fonction en cliquant sur le bouton *Paramètres*, qui se trouve dans le

coin supérieur droit de l'interface principale.

Première étape. **Cliquez** sur

pour activer la fenêtre *RÉGLAGES PRINCIPAUX* d'**avast!**, puis **sélectionnez** *Mises à jour* pour afficher le panneau *RÉGLAGES DES MISES À JOUR*.

Deuxième étape. **Cliquez** sur l'option *Mise à jour manuelle* dans les rubriques MOTEUR ET BASE DE DONNÉES VIRALE VPS et PROGRAMME.

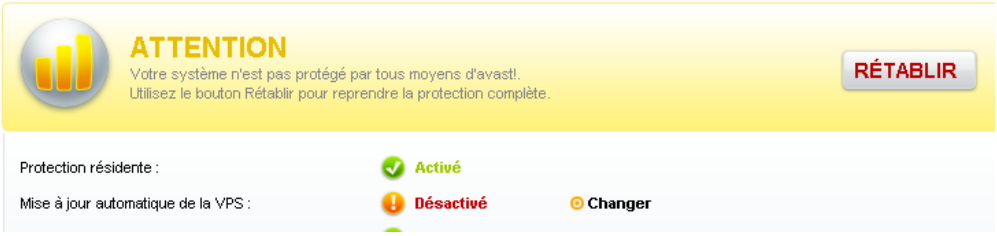


Figure 6: Le panneau RÉSUMÉ ATTENTION indiquant que la Mise à jour automatique de la VPS est désactivée

Les utilisateurs avancés voudront peut-être raffiner davantage leurs réglages dans les rubriques *Détails* et *Réglage du Proxy*. Pour ce faire, suivez les étapes énumérées ci-dessous:

Troisième étape. **Cliquez** sur pour développer les rubriques *Détails* et *Réglage du Proxy* et en modifier les paramètres.

Vous avez appris les différentes méthodes pour mettre à jour manuellement *le moteur et la base de données virale* et le *programme* d'**avast!**. Pour commencer à utiliser **avast!**, veuillez lire attentivement la section **4.0 Comment utiliser avast! pour détecter et éliminer des virus**

Comment utiliser avast! pour détecter et éliminer des virus

Sommaire des sections de cette page:

- **4.0 Avant de commencer**
- **4.1 Comment faire face efficacement à une attaque de virus**
- **4.2 Un survol de l'interface principale d'avast!**
- **4.3 Comment balayer votre ordinateur pour détecter des programmes malveillants et des virus**
- **4.4 Comment exécuter un Scan minutieux du système**
- **4.5 Comment exécuter un Scan de dossiers**
- **4.6 Comment exécuter un Scan au démarrage**
- **4.7 Comment gérer les virus détectés**
- **4.8 Comment utiliser la Zone de quarantaine**
- **4.9 Méthodes avancées de suppression de virus**

4.0 Avant de commencer

Le traitement efficace des virus et logiciels malveillants à l'aide d'**avast!** comporte deux étapes importantes. Il vous faut d'abord balayer (ou scanner) votre ordinateur pour détecter les menaces. Il faut ensuite éliminer les menaces ou les délacer vers la *Zone de quarantaine* d'**avast!**. La suppression et/ou le déplacement des virus et logiciels malveillants empêche ceux-ci d'interagir avec d'autres systèmes, tel que le système de fichiers ou les programmes de gestion du courrier électronique.

Il peut paraître étrange de sauvegarder de tels virus ou logiciels malveillants. Mais si ceux-ci se sont attachés à des données importantes ou sensibles, vous voudrez peut-être ultérieurement récupérer ou sauvegarder ces documents, fichiers ou programmes infectés. Dans de rares cas, **avast!** peut se tromper en identifiant des codes et programmes légitimes comme malveillants. Généralement appelés *faux positifs*, ces codes ou programmes sont potentiellement important pour le bon fonctionnement de votre système, il vous faudra peut-être les récupérer ultérieurement.

La *Zone de quarantaine* d'**avast!** est un espace virtuel où vous pouvez examiner un virus et déterminer s'il constitue une authentique menace, soit en effectuant une recherche sur Internet, soit en le soumettant à l'attention d'un laboratoire spécialisé (une option qui s'offre à vous dans **avast!** en cliquant à droite sur un virus listé dans la *Zone de quarantaine*. Cette opération *n'activera pas* le virus ou le logiciel malveillant en question car la *Zone de quarantaine* l'isole du reste de votre système.

Astuce: À l'inverse, la *Zone de quarantaine* d'**avast!** peut être utilisée pour y transférer des données importantes ou sensibles et les mettre à l'abri en cas d'attaque de virus.

Dans cette section:

- Nous étudierons les pratiques exemplaires pour protéger votre réseau et/ou votre ordinateur personnel;
- Nous explorerons l'interface principale, et en particulier les onglets LANCER UN SCAN et MAINTENANCE;
- Nous verrons comment exécuter les divers types de scans; et
- Nous verrons comment utiliser la *Zone de quarantaine* d'**avast!**.

4.1 Comment faire face efficacement à une attaque de virus

Il y a un ensemble de précautions élémentaires que vous pouvez prendre pour limiter les menaces contre votre ordinateur; par exemple, en évitant les sites douteux ou problématiques ou en utilisant régulièrement des logiciels anti-mouchard et antivirus comme **avast!** et **Spybot**. Cela dit, il est possible que notre système personnel fasse partie d'un réseau local (LAN) et/ou que l'on partage une connexion Internet. Les considérations qui suivent concernent les façons de réagir efficacement à une attaque de virus lorsque plusieurs ordinateurs sont en réseau, que ce soit en contexte communautaire ou au travail.

- Déconnectez physiquement votre ordinateur d'Internet et du réseau local. Si vous utilisez une connexion sans fil, déconnectez votre ordinateur du réseau sans fil. Si possible, éteignez la machine et retirez la carte de communications sans fil.
- Si votre ordinateur fait partie d'un réseau, vous devriez immédiatement déconnecter tous les ordinateurs d'Internet et du réseau lui-même. Chaque utilisateur devrait cesser d'utiliser le réseau et lancer **avast!** ou un autre programme antivirus fiable afin de détecter et éliminer le virus. Cela peut sembler laborieux, mais cette procédure est essentielle à la protection des ordinateurs personnels et du réseau.
- Planifiez un Scan au prochain démarrage pour chaque ordinateur du réseau. Notez bien le nom de chaque virus détecté, de sorte que vous puissiez effectuer une recherche, puis supprimez-les ou déplacez-les vers la *Zone de quarantaine* d'**avast!**. Pour vous familiariser avec cette procédure, veuillez consulter la section **4.6 Comment exécuter un Scan au démarrage**.
- Même si un virus a été détecté ou réparé, répétez les étapes précédentes et lancez un scan au démarrage sur *chaque* ordinateur, jusqu'à ce qu'**avast!** n'affiche plus aucun message d'avertissement. Selon la gravité de l'attaque, il est possible qu'un seul scan au démarrage suffise.

Pour plus de renseignements sur les moyens de défense contre les virus et les logiciels malveillants, veuillez consulter la section **4.9 Méthodes avancées de suppression de virus**

4.2 Un survol de l'interface principale d'avast!

L'interface utilisateur d'**avast!** comporte quatre onglets principaux, situés à la gauche de la fenêtre: RÉSUMÉ, LANCER UN SCAN, PROTECTION RÉSIDENTE et MAINTENANCE. Chaque onglet est divisé en sous-onglets qui permettent d'afficher les panneaux correspondants.

Première étape. **Cliquez** sur pour afficher la fenêtre ci-dessous:

avast! ANTIVIRUS GRATUIT
CENTRE D'AIDE
PARAMÈTRES
METTRE À NIVEAU
RÉSUMÉ
État actuel
Statistiques
LANCER UN SCAN
PROTECTION RÉSIDENTE
MAINTENANCE
SÉCURISÉ
Votre système est protégé par tous les moyens d'avast!.
Moins de détails...
Protection résidente : Activé
Mise à jour automatique de la VPS : Activé
Version de la base de données virale VPS : 110117-1
Version du programme : 5.1.889
Date d'expiration : 2011-08-17 18:14:21
MODE SILENCIEUX : DÉSACTIVÉ
Activer
avast! va afficher ses messages/pop-up/alertes et sons si nécessaire, mais restera silencieux si une application en plein écran est active.
Modifier les réglages

Figure 1: L'onglet RÉSUMÉ affichant le panneau État actuel SÉCURISÉ

La liste ci-dessous détaille brièvement les fonctions des quatre onglets principaux:

RÉSUMÉ: Cet onglet comprend les sous-onglets *État actuel* et *Statistiques*. Le sous-onglet *État actuel* affiche l'état des composantes principales utilisées par **avast!** pour défendre votre ordinateur contre les virus et autres attaques. Le panneau *Statistiques* affiche les opérations des composantes d'**avast!**. Affichage par semaine, mois ou année.

LANCER UN SCAN: Cet onglet comporte les sous-onglets *Scanner maintenant*, *Scan au démarrage* et *Rapports de scans*. Le panneau *SCANNER MAINTENANT* affiche les différentes options de scan manuels. Le panneau *SCAN AU DÉMARRAGE* vous permet de planifier un scan au prochain démarrage de votre ordinateur. Le panneau *RAPPORTS DE SCANS* affiche un rapport des scans manuels effectués, sous forme de tableau.

PROTECTION RÉSIDENTE: Cet onglet affiche tous les agents de protection associés aux fonctions de votre ordinateur, dont l'*AGENT DES FICHIERS*. Vous avez ici un accès direct aux réglages des agents de protection, y compris les boutons pour les arrêter et les démarrer.

MAINTENANCE: Cet onglet comporte les sous-onglets *Mise à jour*, *Enregistrement*, *Zone de quarantaine* et *À propos d'avast!*. Le panneau *MISE À JOUR* vous permet de lancer manuellement des mises à jour du programme et des définitions de virus. Le panneau *ENREGISTREMENT* vous permet d'enregistrer votre copie d'**avast!**. Le panneau *ZONE DE QUARANTAINE* affiche les virus et logiciels malveillants détectés par **avast!** lors des scans et vous permet de les gérer de différentes façons, soit en les supprimant, en lançant de nouveaux scans ou en soumettant les virus détectés à l'analyse de laboratoires spécialisés. Le panneau *À PROPOS D'AVAST* affiche des renseignements sur la plus récente version d'**avast!** installée sur votre ordinateur.

Commentaire: Les panneaux *LANCER UN SCAN* et *MAINTENANCE* sont particulièrement pratiques pour traiter les menaces posées par des virus et des logiciels malveillants.

4.3 Comment balayer votre ordinateur pour détecter des programmes malveillants et des virus

Dans cette section, nous examinerons les différentes options de scan disponibles, ainsi que leur mode d'emploi. Nous verrons également comment lancer un scan du système, un scan de dossiers et un scan au démarrage.

Le panneau *LANCER UN SCAN > SCANNER MAINTENANT* présente les quatre options de scan offertes par **avast!**; pour les afficher, suivez les étapes décrites ci-dessous:

Première étape. **Cliquez** sur

pour afficher la fenêtre suivante:

avast! ANTIVIRUS GRATUIT
CENTRE D'AIDE
PARAMÈTRES
METTRE À NIVEAU
RÉSUMÉ
LANCER UN SCAN
Scanner maintenant
Scan au démarrage
Rapports de scans
PROTECTION RÉSIDENTE
MAINTENANCE
SCANNER MAINTENANT
Utilisez les contrôles ci-dessous pour lancer un des scans prédéfinis ou créer un scan personnalisé selon vos préférences. Plusieurs scans peuvent être lancés en même temps.
Scan rapide
Scan rapide de la mémoire vive et des disques durs.
Démarrer
Plus de détails
Scan minutieux
Scan méticuleux du système (précis mais plus lent).
Démarrer
Plus de détails
Scan des médias amovibles
Scan des médias amovibles (CDs, DVDs et similaires) actuellement présents dans l'ordinateur.
Démarrer
Plus de détails
Scan des dossiers sélectionnés
Scan minutieux des dossiers sélectionnés (à sélectionner au démarrage du scan).
Démarrer
Moins de détails

Figure 2: L'onglet LANCER UN SCAN affichant le panneau SCANNER MAINTENANT

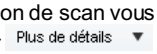
Les descriptions suivantes vous aideront à choisir le mode de scan le plus approprié:

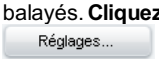
Scan rapide: Cette option est recommandée aux utilisateurs qui ont peu de temps pour détecter de potentielles menaces.

Scan minutieux: Cette option est recommandées aux utilisateurs qui ont assez de temps pour lancer un scan minutieux de leur système. Ce mode est également recommandé si vous utilisez le programme antivirus pour la première fois sur votre ordinateur. La durée de ce scan dépend du nombre de documents, de fichiers, de dossiers et de disques durs sur votre ordinateur, ainsi que la vitesse de la machine. Veuillez consulter la section **4.4 Comment exécuter un Scan minutieux du système**.

Scan des médias amovibles: Cette option est recommandée pour scanner des disques durs externes, des clés USB et d'autres dispositifs ou supports amovibles, en particulier ceux qui ne vous appartiennent pas. **avast!** tentera de détecter des programmes malveillants conçus pour s'exécuter lorsque le dispositif est connecté.

Scan des dossiers sélectionnés: Cette option est recommandée pour scanner un ou plusieurs dossiers en particulier. Cette option est utile si vous soupçonnez qu'un fichier ou un dossier est infecté. Veuillez consulter la section **4.5 Comment exécuter un Scan de dossiers**.

Astuce: Chaque option de scan vous permet de voir les détails du scan, par exemple, les secteurs qui sont actuellement balayés. **Cliquez** sur 

pour les afficher. Si vous êtes un utilisateur avancé ou expert, **cliquez** sur 

pour raffiner les réglages pour chaque mode de scan.

4.4 Comment exécuter un Scan minutieux du système

Pour lancer un scan minutieux du système, suivez les étapes décrites ci-dessous:

Première étape. **Cliquez** sur dans la rubrique du mode *Scan minutieux* pour afficher la fenêtre suivante:

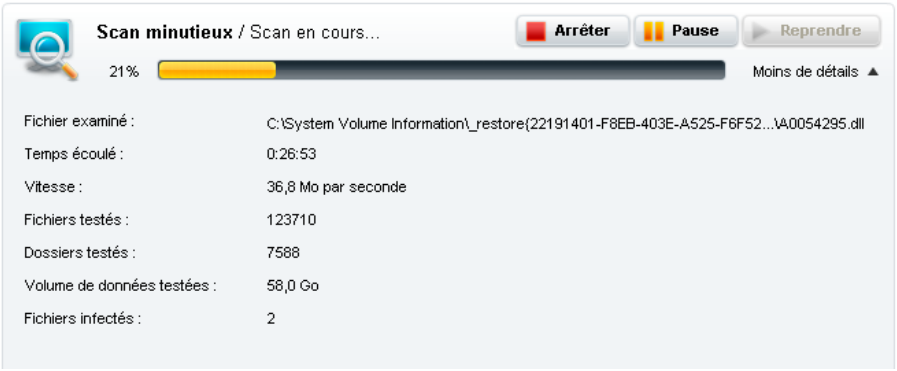


Figure 3: Le panneau SCANNER MAINTENANT affichant le scan minutieux en cours d'exécution

À l'issue du scan minutieux, si une menace a été détectée sur votre ordinateur le panneau *Scan minutieux* ressemblera à ceci:

Figure 4: La rubrique Scan complété affichant un avertissement MENACE DÉTECTÉE!

Le scan minutieux du système a détecté quelques menaces; pour savoir quoi faire à partir de là, veuillez consulter la section **4.7 Comment gérer les virus détectés**.

La *Zone de quarantaine* d'**avast!** est un dossier mis en place lors du processus d'installation d'**avast!**; c'est une zone de quarantaine virtuelle où les virus et les logiciels malveillants sont isolés de telle sorte qu'ils ne peuvent pas interagir avec, ou parasiter, les autres processus en cours sur votre ordinateur.

4.5 Comment exécuter un Scan de dossiers

Pour scanner vos dossiers, suivez les étapes décrites ci-dessous:

Première étape. **Cliquez** sur dans la rubrique du mode *Scan des dossiers sélectionnés* pour afficher la fenêtre suivante:

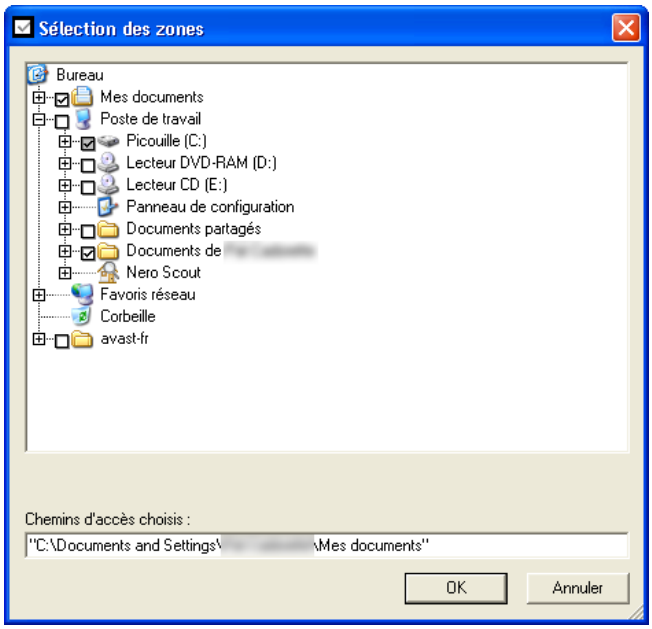


Figure 5: La boîte de dialogue Sélection des zones

La boîte de dialogue *Sélection des zones* vous permet de choisir le dossier que vous souhaitez scanner. Vous pouvez également sélectionner plus d'un dossier. Lorsque vous cochez la case correspondant à chaque dossier, le chemin d'accès du dossier s'affiche dans le champs *Chemins d'accès choisis:*.

Deuxième étape. **Cliquez** sur OK pour lancer le scan de vos dossiers et afficher la fenêtre suivante:

Figure 6: Le Scan de dossiers en cours d'exécution

Astuce: **avast!** vous permet de scanner des dossiers à partir du menu local *Windows* standard qui s'affiche lorsque vous cliquez à droite sur un dossier donné. Vous n'avez qu'à **sélectionner** l'icone qui apparaît à côté du nom du dossier que vous souhaitez scanner.

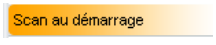
4.6 Comment exécuter un Scan au démarrage

Le scan au démarrage d'**avast!** vous permet de planifier un scan complet de votre disque dur avant que le *Système d'exploitation Windows de Microsoft* ne soit mis en exécution. Au moment où le scan au démarrage s'exécute, la majorité des programmes malveillants sont toujours en dormance, c'est-à-dire, qu'ils n'ont pas encore eu l'occasion de s'activer ou d'interagir avec d'autres processus du système. C'est pourquoi ils sont plus facilement détectables à cette étape.

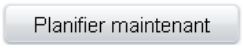
Le scan au démarrage accède directement au disque sans passer par les pilotes du système de fichier **Windows**, une cible de premier choix pour la plupart des programmes malveillants. Un scan au démarrage devrait être en mesure de détecter même les plus agressifs des "rootkits" (c'est le nom employé pour désigner un type de logiciel malveillant particulièrement pernicieux). Il est **fortement recommandé** de planifier un scan au démarrage si vous avez le moindre soupçon que votre système a été compromis ou infecté.

L'option *Scan au démarrage* est recommandée pour un scan complet et minutieux de votre système. Le scan peut prendre un certain temps, selon la vitesse de votre ordinateur, la quantité de données à examiner et le nombre de disques dur branchés à votre ordinateur. Le *Scan au démarrage* est toujours planifié pour le prochain redémarrage de votre ordinateur.

Pour scanner votre système au prochain démarrage, suivez les étapes décrites ci-dessous:

Première étape. **Cliquez** sur 

pour afficher le panneau *SCAN AU DÉMARRAGE*.

Deuxième étape. **Cliquez** sur 

pour planifier un scan au prochain démarrage de votre ordinateur.

Troisième étape. **Cliquez** sur

pour lancer le scan au démarrage immédiatement si vous préférez.

Commentaire: Un scan au démarrage s'exécute avant que le système d'exploitation et l'interface utilisateur ne soient chargés. C'est pourquoi vous ne verrez qu'un écran bleu affichant le progrès du scan, tel qu'illustré ci-dessous:

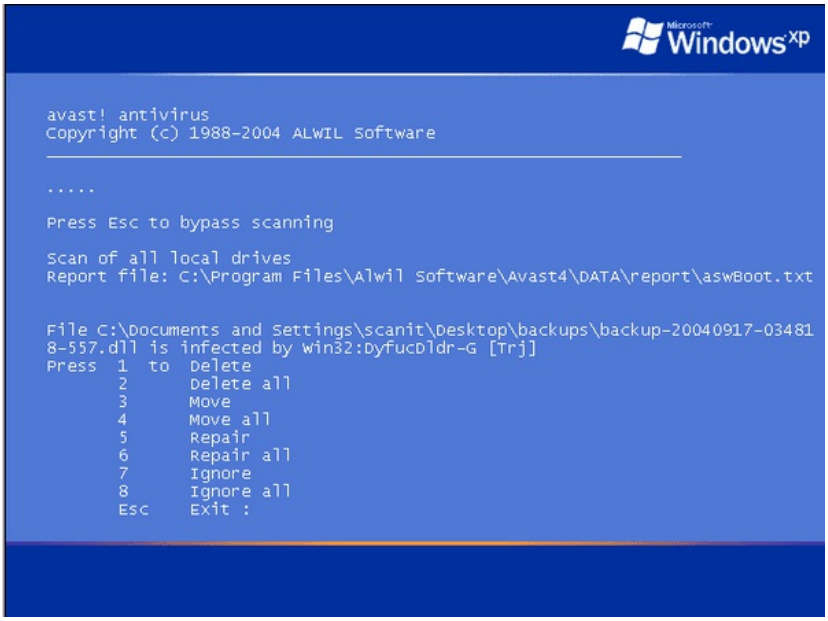


Figure 7: Le scan au démarrage planifié d'avast!

Chaque fois qu'**avast!** détecte une menace, le programme vous demande si vous voulez *Supprimer*, *Ignorer*, *Mettre en quarantaine* ou *Réparer* les virus détectés. Il est recommandé de ne *jamais* les ignorer. La liste de ces commandes n'apparaît uniquement que si un virus est détecté sur votre système.

4.7 Comment gérer les virus détectés

Lors du processus d'installation d'**avast!**, la *Zone de quarantaine* d'**avast!** a été créée sur votre disque dur. La *Zone de*

quarantaine n'est ni plus ni moins qu'un dossier qui est isolé du reste de votre système et utilisé pour stocker les logiciels malveillants ou les virus détectés au cours du scan, ainsi que les documents, fichiers et dossiers infectés ou compromis.

Si vous avez déjà mis à jour le programme et la base de données virale, vous êtes déjà familier avec l'onglet *MAINTENANCE*, par lequel vous pouvez également accéder à la *Zone de quarantaine* d'**avast!**.

Pour gérer adéquatement les virus et logiciels malveillants détectés lors du scan, suivez les étapes décrites ci-dessous:

Première étape. **Cliquez** sur AFFICHER LES RÉSULTATS pour afficher la fenêtre suivante:

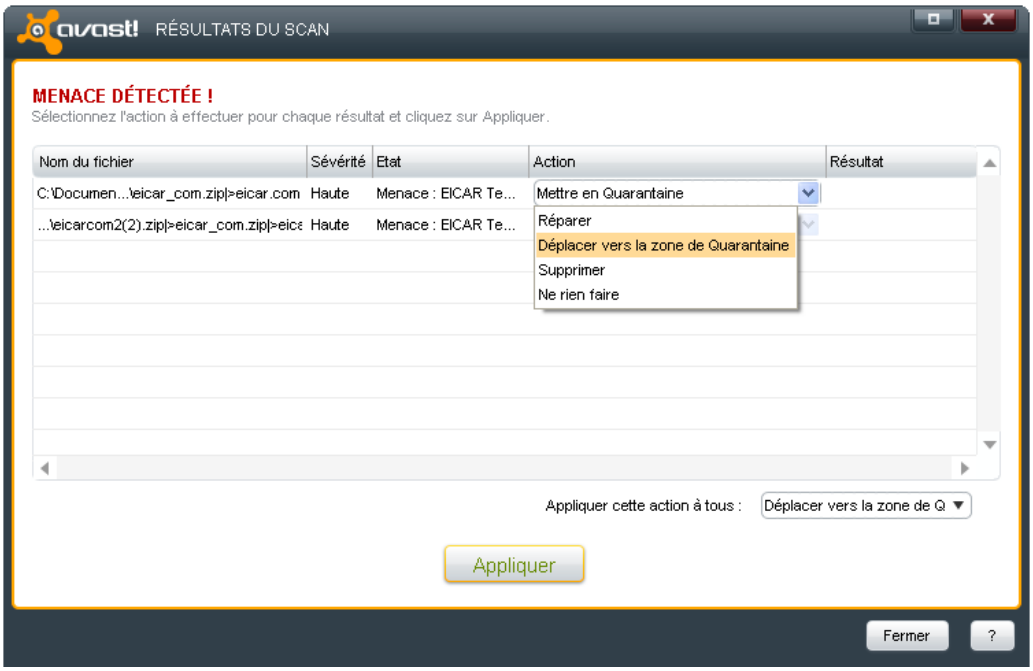


Figure 8: La fenêtre RÉSULTATS DU SCAN affichant le message d'avertissement MENACE DÉTECTÉE!

Deuxième étape. **Cliquez** sur Action pour afficher le menu déroulant présentant la liste des actions qui peuvent être appliquées aux menaces détectées, tel qu'illustré à la *Figure 8*, ci-dessus.

Commentaire: Dans cet exercice, nous voulons déplacer les fichiers infectés vers la *Zone de quarantaine*. Cependant, le menu déroulant présente trois autres options que nous décrivons sommairement ci-dessous:

Réparer: Cette action tentera de réparer le fichier infecté.

Supprimer: Cette action supprimera de façon permanente le fichier infecté.

Ne rien faire: Cette action *n'est définitivement pas recommandée* lorsqu'il est question de gérer adéquatement des virus ou des programmes malveillants.

Troisième étape. **Sélectionnez** l'action *Déplacer vers la zone de quarantaine*, puis **cliquez** sur Appliquer pour afficher la fenêtre ci-dessous:

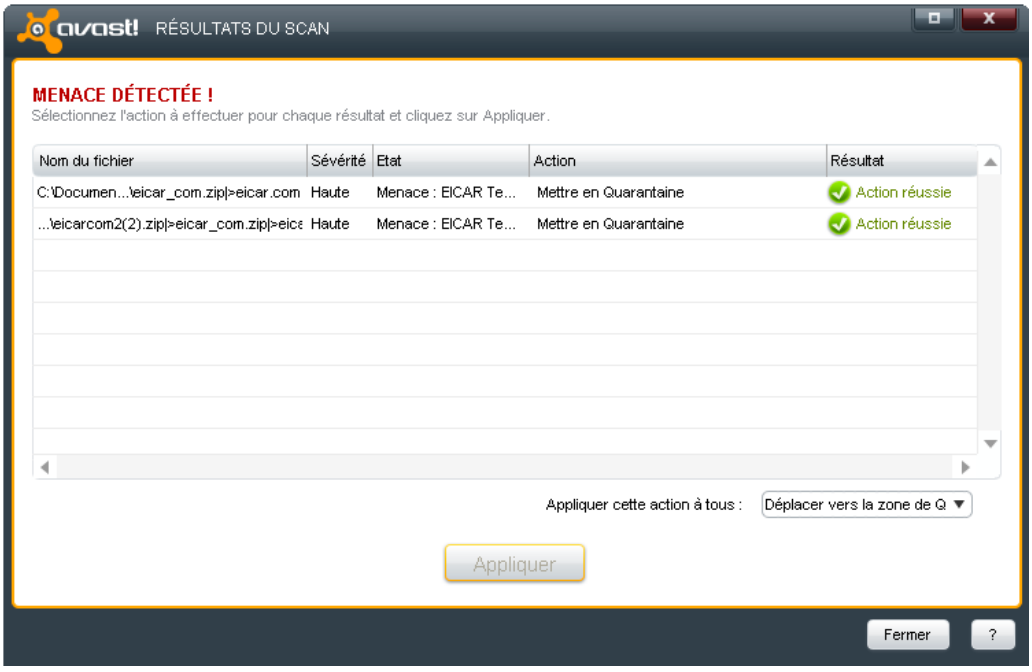


Figure 9: Les virus ont été déplacés vers la Zone de quarantaine

4.8 Comment utiliser la Zone de quarantaine

Maintenant que le virus a été délacé vers la *Zone de quarantaine* d'**avast!**, vous pouvez déterminer quelle est la meilleure chose à faire.

Première étape. **Cliquez** sur

puis **cliquez** sur

pour afficher la fenêtre ci-dessous:

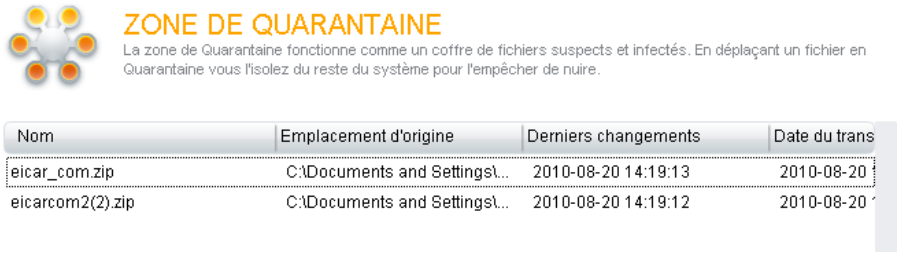


Figure 10: La Zone de quarantaine affichant deux virus

Deuxième étape: **Cliquez à droite** sur un des virus pour afficher le menu des actions possibles, tel qu'illustré ci-dessous:

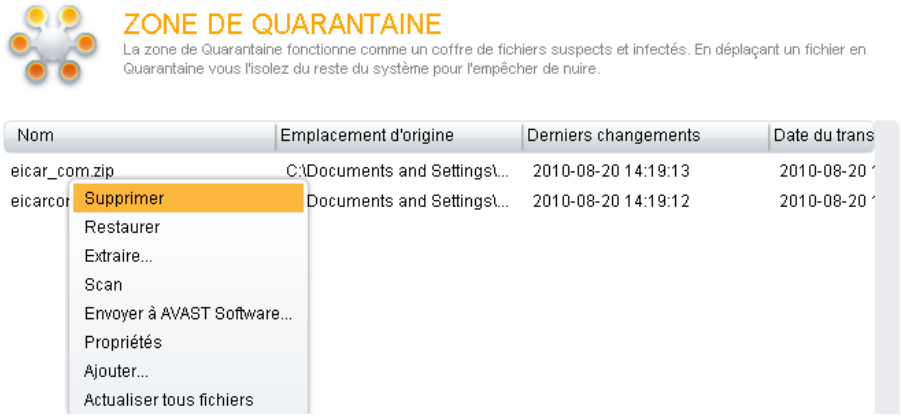


Figure 11: Le menu déroulant des actions à appliquer aux virus dans la Zone de quarantaine

Commentaire: Vous n'activerez pas un virus en double-cliquant dessus dans la *Zone de quarantaine*. Cette action affichera plutôt les propriétés du virus, de la même façon que si vous cliquiez sur l'option *Propriétés* dans le menu local.

La liste ci-dessous décrit les différentes actions du menu déroulant:

Supprimer: Cette action supprimera le virus de façon irréversible.

Restaurer: Cette action restaurera les virus à leur emplacement initial.

Extraire...: Cette action copiera le fichier ou le virus dans un dossier de votre choix.

Scan: Cette action soumettra le virus à un nouveau scan.

Envoyer à AVAST Software...: Cette action vous permet de soumettre le virus à une analyse plus poussée. En sélectionnant cette action, vous activerez un formulaire à remplir et à envoyer.

Propriétés: Cette action vous permet d'afficher plus de détails concernant le virus en question.

Ajouter...: Cette action vous permet de naviguer dans votre système pour chercher d'autres fichiers que vous aimeriez déplacer vers la *Zone de quarantaine*. Cette fonction pourrait s'avérer très utile pour protéger certains fichiers lors d'une attaque de virus.

Actualiser tous fichiers: Cette action permet d'opérer une mise à jour des fichiers pour être certain d'afficher les fichiers les plus récents.

4.9 Méthodes avancées de suppression de virus

Dans certains cas, la protection fournie par **avast!**, **Comodo Firewall** et **Spybot** n'est tout simplement pas suffisante. Malgré nos efforts les plus rigoureux, nos ordinateurs personnels et de travail sont parfois infectés par des programmes malveillants et des virus. Dans la section **4.1 Comment faire face efficacement à une attaque de virus**, nous avons vu quelques méthodes pour faire face aux virus les plus coriaces. Mais il existe d'autres mesures qui peuvent être mises en place pour éliminer complètement ces menaces.

Méthode A: Utiliser des CD/DVD de secours anti-logiciel malveillant (Rescue CD)

Certaines des compagnies qui développent des outils contre les programmes malveillants offrent également des CD/DVD de secours, ou Rescue CD/DVD. On peut les télécharger sous forme d'images ISO (un format qui peut être facilement gravé sur un disque CD ou DVD).

Pour utiliser un CD ou un DVD anti-programme malveillant, veuillez suivre les étapes décrites ci-dessous:

1. Téléchargez et gravez le programme anti-logiciel malveillant sur un CD. *Vous pouvez utiliser un logiciel gratuit comme **ImgBurn** [15] pour graver l'image sur un disque.*

2. Insérez le disque dans le lecteur de CD/DVD de l'ordinateur infecté, puis redémarrez l'ordinateur à partir du CD/DVD. *Habituellement, vous pouvez démarrer à partir d'un disque en appuyant sur la touche F10 ou F12 du clavier immédiatement après avoir allumé l'ordinateur. Soyez très attentif aux consignes qui s'affichent sur l'écran lors du démarrage pour connaître la méthode appropriée sur votre ordinateur.*

3. Connectez votre ordinateur à Internet pour permettre au programme anti-logiciel malveillant de mettre à jour ses définitions de virus, si nécessaire. Le programme se mettra automatiquement à la recherche des menaces sur votre ordinateur, puis il les supprimera au fur et à mesure.

Voici une liste d'images de CD de secours:

- **AVG Rescue CD** [16]
- **Kaspersky Rescue CD** [17]
- **F-Secure Rescue CD** [18]
- **BitDefender Rescue CD** [19]

Il peut aussi être utile de scanner votre ordinateur à l'aide des outils suivants, qui se mettent en marche au démarrage de **Windows OS**. Par contre, ces outils ne s'exécuteront que si les virus qui infectent votre ordinateur ne les empêchent pas de fonctionner normalement.

- **HijackThis** [20] et d'autres outils gratuits Clean-up Tools [21] de la compagnie **Trend Micro**.
- **RootkitRevealer** [22] de Sysinternals [23] de **Microsoft**.

Commentaire: Il est possible d'utiliser les outils listés ci-dessus séparément pour maximiser vos chances de nettoyer votre ordinateur complètement.

Méthode B: Réinstaller le système d'exploitation Windows de Microsoft

***Commentaire**: Avant d'entamer le processus de réinstallation, assurez vous de disposer de tous les numéros de série et licences nécessaires, ainsi que des copies d'installation de **Windows OS** et de tous les programmes dont vous avez besoin. Ce processus peut prendre un certain temps mais en vaut l'effort si vous n'avez pas réussi à éliminer toutes les menaces avec les autres méthodes.*

Dans de rares cas, une infection peut s'avérer tellement destructrice que les logiciels recommandés ci-dessus s'avèrent impuissants. Dans de telles situations, il est recommandé de suivre les étapes énumérées ci-dessous:

1. Créer une copie de sauvegarde de tous vos fichiers personnels.

2. Réinstaller le système d'exploitation **Microsoft Windows** en formatant le disque au complet.

3. Mettre à jour le système d'exploitation **Microsoft Windows** immédiatement après l'installation.

4. Installer **avast!** (ou un autre programme antivirus recommandé) et le mettre à jour.

5. Installer tous les programmes dont vous avez besoin et télécharger les plus récentes versions, ainsi que toutes les mises à jour pour chaque programme.

   IMPORTANT: Vous ne devriez *jamais* insérer votre disque de sauvegarde dans le lecteur de votre ordinateur *avant* d'avoir compléter toutes ces tâches. Vous risqueriez ainsi de ré-infecter votre ordinateur.

6. Insérez votre copie de sauvegarde dans le lecteur de l'ordinateur et exécutez un scan minutieux pour détecter et éliminer tous les problèmes potentiels.

7. Lorsque vous aurez détecté et supprimé tous les problèmes, vous pourrez copier vos fichiers du disque de sauvegarde vers votre disque dur.

Faq et questions récapitulatives

Elena et Nikolai trouvent Avast plutôt facile à utiliser, mais ils ne sont pas encore certains de connaître assez bien le programme et ses fonctionnalités.

Q: *Comment puis-je m'assurer que mes documents ne seront pas infectés si j'utilise un ordinateur dans un café Internet, et qu'aucun programme antivirus n'est installé sur cet ordinateur?*

A: *Excellente question! Il est bon de constater que tu te rends compte à quel point les virus peuvent s'avérer dangereux. L'utilisation d'ordinateurs publics comporte un facteur de risque élevé. On ne sait jamais quel type de programmes malveillants peuvent s'y trouver. Voici un conseil simple : ne jamais utiliser d'ordinateurs publics pour effectuer des tâches importantes ou délicates, à moins de n'avoir absolument aucune alternative.*

Q: *J'ai plusieurs ordinateurs et une connexion Internet plutôt lente. Comment puis-je télécharger la mise à jour des définitions de virus pour tous mes ordinateurs?*

A: *Tu peux **télécharger les plus récentes mises à jour** [24] directement du site Internet d'avast!, puis les distribuer à chaque ordinateur de ton réseau.*

Q: *Qu'advient-il des fichiers qui se trouvent dans la Zone de quarantaine si je désinstalle **avast!**?*

A: *Tous les fichiers contenus dans la Zone de quarantaine seront supprimés si tu désinstalles le programme.*

5.1 Questions récapitulatives

- Comment peut-on scanner un répertoire en particulier avec **avast!**?
- Combien de jours peut-on utiliser **avast!** avant de devoir l'enregistrer?
- Est-il possible de déplacer un document qui n'est pas infecté par un virus vers la *Zone de quarantaine*?
- Quelle est la différence entre supprimer un virus et le déplacer vers la *Zone de quarantaine*?
- Quelle est la différence entre un scan au démarrage et un scan minutieux du système?

Spybot - anti-mouchard

Short Description:

Spybot Search & Destroy est utilisé pour détecter et éliminer divers types de logiciels publicitaires (*adware*), malveillants (*malware*) ou espions (*spyware*). Le programme offre des mises à jour gratuites et vous permet d'immuniser votre navigateur Internet contre des infections futures.

Online Installation Instructions:

Pour télécharger Spybot

- *Lisez la courte **introduction** aux **Guides pratiques** [1].*
- ***Cliquez** sur l'icone **Spybot**ci-dessous pour ouvrir la page de téléchargement **http://www.safer-networking.org/fr/mirrors/index.html***
- *Choisissez une source de téléchargement parmi celles listées su cette page en cliquant sur le bouton "**Téléchargement ici**".*
- *Téléchargez le programme d'installation. Ensuite, trouvez-le et cliquez dessus.*
- *Si vous avez sauvegardé l'exécutable de **Spybot** sur votre ordinateur, vous pouvez le supprimer après l'installation.*

Spybot:
[25]

Site Internet

www.safer-networking.org/fr [26]

Configuration requise

- Compatible avec toutes les versions de Windows

Version utilisée pour rédiger ce guide

- 1.6.2

Licence

- Gratuiciel (*Freeware*)

Lecture requise

- Livret pratique Security in-a-box, chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** [4]

Niveau: 1: Débutant, **2 : Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

Temps d'apprentissage: 20 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de **supprimer** plusieurs types de logiciels malveillants et/ou espions.
- La capacité de **vacciner** votre système informatique **avant** qu'il ne soit infecté ou menacé de perturbations malveillantes.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Les systèmes d'exploitation **GNU Linux** et **Mac OS** sont, à l'heure actuelle, pratiquement épargnés par les logiciels malveillants (mouchards, virus, etc.). Pour vous protéger, nous vous recommandons de: **1)** mettiez régulièrement à jour votre système d'exploitation, ainsi que tous les programmes qui y sont installés; **2)** utilisez un des programmes antivirus listés au chapitre portant sur *Avast* [27]; **3)** utilisiez un des programme pare-feu listés au chapitre portant sur *Comodo* [28]; **4)** utilisiez un navigateur sûr comme *Firefox* [29] avec le module complémentaire [*NoScript*] (/fr/firefox_noscript) qui empêche l'exécution des scripts téléchargés automatiquement avec les pages web. Ces mesures préventives suffiront à protéger votre système **GNU Linux** ou **Mac OS**.

La situation est très différente pour les ordinateurs équipés du système **Microsoft Windows**. Des milliers de nouveaux logiciels malveillants sont conçus chaque jour. Les méthodes d'attaque sont de plus en plus sophistiquées. Les mesures préventives décrites au précédent paragraphe sont **nécessaires** aux ordinateurs qui fonctionnent avec **Microsoft Windows**. De plus, nous recommandons fortement l'utilisation de **Spybot**, telle que décrite dans le présent chapitre. Si malgré toutes ces précautions votre ordinateur est infecté et que vous avez besoin d'outils supplémentaires, nous recommandons les logiciels suivants:

1. Installez **SuperAntiSpyware** [30], actualisez les définitions et scannez votre ordinateur.
2. Installez **Malwarebytes Anti-Malware** [31], lancez un *Scan rapide*, puis lancez un *Scan*. Lorsque l scan est complété, supprimez les mouchards détectés affichés dans le panneau *Show Results*
3. Utilisez d'autres programmes anti-mouchards gratuits comme: **Microsoft Windows Defender** [32], **Ad-Aware Internet Security** [33] ou **SpywareBlaster** [34].

1.1 À propos de cet outil

Spybot S&D est un programme libre et gratuit, dont l'usage est très répandu pour détecter et éliminer des systèmes informatiques divers types de logiciels publicitaires (*adware*), malveillants (*malware*) ou espions (*spyware*). Le programme vous permet également de vacciner votre système contre les logiciels publicitaires, malveillants et/ou espions avant même qu'ils n'infectent votre ordinateur.

Le terme « logiciel publicitaire » (ou publiciel; *adware* en anglais) désigne tout logiciel qui affiche des publicités sur votre ordinateur. Certains types de publiciels fonctionnent sensiblement comme des logiciels espions et peuvent envahir votre vie privée ou menacer la sécurité de votre système.

Le terme « logiciel malveillant » (*malware* en anglais) désigne tout programme – par ex. des Chevaux de Troie (*Trojans*) ou des vers informatiques (*worms*) – conçu pour nuire à votre ordinateur ou en détourner les opérations sans votre consentement, ou sans même que vous en soyez conscient.

Le terme « logiciel espion » (ou mouchard; *spyware* en anglais), désigne tout programme conçu pour récolter des données, observer et enregistrer vos renseignements privés et surveiller vos habitudes de navigation sur Internet. Tout comme les logiciels malveillants, les mouchards s'exécutent souvent sur votre ordinateur à votre insu. C'est pourquoi l'installation d'un programme comme **Spybot** vous aidera à protéger votre système et à VOUS protéger!

Spybot installe aussi une application supplémentaire appelée **TeaTimer**. Cela protégera votre ordinateur contre d'éventuelles infections par des logiciels malveillants.

Commentaire: **Windows Vista** comporte son propre programme anti-espion, appelé **Windows Defender**. **Vista** semble cependant laisser **Spybot** fonctionner sans conflit.

Comment installer et utiliser Spybot

Sommaire des sections de cette page:

- **2.0 Comment installer Spybot**
- **2.1 À propos de Spybot**
- **2.2 Comment utiliser Spybot pour la première fois**
- **2.3 Comment actualiser les règles de détection et les bases de données de vaccination de Spybot**
- **2.4 Comment vacciner votre système**
- **2.5 Comment détecter la présence de problèmes**
- **2.6 Le Résident TeaTimer**
- **2.7 Comment utiliser l'outil de Sauvegardes**

2.0 Comment installer Spybot

Première étape. **Double-cliquez** sur spybotsd162.exe; si la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, **cliquez** sur Exécuter pour afficher la fenêtre suivante:

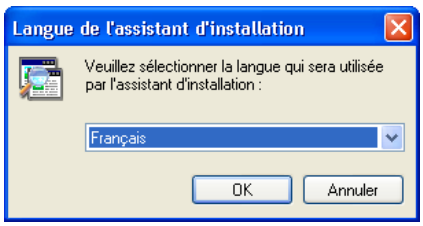


*Figure 1: La fenêtre Langue de l'assistant d'installation *

Deuxième étape. **Cliquez** sur OK pour afficher la fenêtre *Installation - Spybot Search & Destroy – Bienvenue dans l'assistant d'installation de Spybot - Search & Destroy*.

Troisième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Accord de licence*. Veuillez lire l'*Accord de licence* avant de poursuivre le processus d'installation.

Quatrième étape. **Cochez** l'option *Je comprends et j'accepte les termes du contrat de licence* pour activer le bouton *Suivant*, puis **cliquez** sur Suivant > pour afficher la fenêtre *Dossier de destination*.

Cinquième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

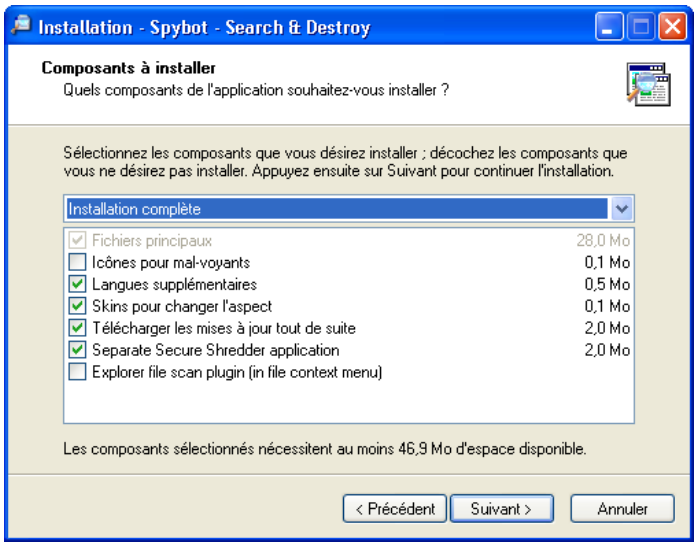

Installation - Spybot - Search & Destroy
Composants à installer
Quels composants de l'application souhaitez-vous installer ?
Sélectionnez les composants que vous désirez installer ; décochez les composants que vous ne désirez pas installer. Appuyez ensuite sur Suivant pour continuer l'installation.
Installation complète
Fichiers principaux 28,0 Mo
Icônes pour mal-voyants 0,1 Mo
Langues supplémentaires 0,5 Mo
Skins pour changer l'aspect 0,1 Mo
Télécharger les mises à jour tout de suite 2,0 Mo
Separate Secure Shredder application 2,0 Mo
Explorer file scan plugin (in file context menu)
Les composants sélectionnés nécessitent au moins 46,9 Mo d'espace disponible.
< Précédent
Suivant >
Annuler

Figure 2: La fenêtre Composants à installer

Sixième étape. **Cochez** les composants appropriés pour que la fenêtre correspondent à la *figure 2* ci-dessous, puis **cliquez** sur Suivant > pour afficher la fenêtre *Sélection du dossier de menu Démarrer*.

Septième étape. **Cliquez** sur Suivant > pour accepter l'emplacement par défaut et afficher la fenêtre *Tâches supplémentaires*.

Huitième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Prêt à installer*, puis **cliquez** sur Installer pour afficher la fenêtre *Installation en cours*.

Neuvième étape. **Cliquez** sur Terminer pour finaliser le processus d'installation et lancer **Spybot - Search & Destroy**.

2.1 À propos de Spybot

L'utilisation appropriée de **Spybot** comporte deux étapes élémentaires:

- Mettre à jour les *Règles de détection* (*Detection Rules*) et les *Bases de données de vaccination* (*Immunization databases*) avec l'information la plus récente et la plus pertinente.
- Exécuter **Spybot**. Cela implique la vaccination de votre système avec les règles de détection et les bases de données de vaccination que vous avez préalablement téléchargées, la vérification du système afin de détecter tout logiciel malveillant ou espion qui pourrait s'y trouver et, finalement, l'élimination des infections trouvées.

Note: Pour un aperçu des fonctions avancées, veuillez consulter la section **3.0 Mode avancé** [35].

2.2 Comment utiliser Spybot pour la première fois

Lorsque vous aurez finalisé l'installation, **Spybot** *affichera automatiquement la fenêtre* Infos légales *illustrée ci-dessous*:

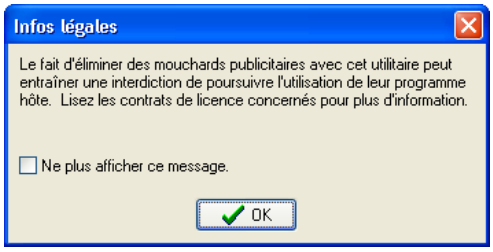

Infos légales
Le fait d'éliminer des mouchards publicitaires avec cet utilitaire peut entraîner une interdiction de poursuivre l'utilisation de leur programme hôte. Lisez les contrats de licence concernés pour plus d'information.
Ne plus afficher ce message.
OK

Figure 3: La fenêtre Infos légales

Commentaire: Pour lancer **Spybot** la prochaine fois, vous pouvez, soit **double- cliquer** sur ou **sélectionner Démarrer > Programmes > Spybot - Search & Destroy > Spybot - Search & Destroy.**

Première étape. **Cliquez** sur OK pour afficher la console *Spybot - Search & Destroy* (*figure 8*) et la fenêtre *Créer une sauvegarde du Registre*, tel qu'illustré ci-dessous:

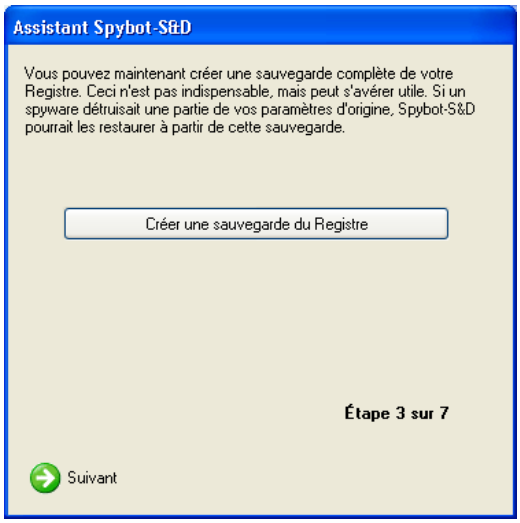

Assistant Spybot-S&D
Vous pouvez maintenant créer une sauvegarde complète de votre Registre. Ceci n'est pas indispensable, mais peut s'avérer utile. Si un spyware détruisait une partie de vos paramètres d'origine, Spybot-S&D pourrait les restaurer à partir de cette sauvegarde.
Créer une sauvegarde du Registre
Étape 3 sur 7
Suivant

Figure 4: La fenêtre Créer une sauvegarde du Registre de l'Assistant Spybot-S&D

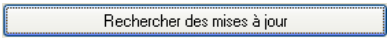
Commentaire: Il est fortement conseillé de créer une copie de sauvegarde du registre. L'explication détaillée du **Registre Windows** est donnée dans le guide pratique **CCleaner** [36].

Deuxième étape. **Cliquez** sur

dans la *figure 4* pour créer et sauvegarder une copie de sauvegarde du registre de votre système.

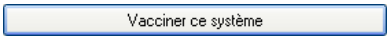
Troisième étape. **Cliquez** sur

pour afficher la fenêtre *Spybot – Rechercher des mises à jour*. Si vous êtes connecté à Internet, suivez les étapes énumérées ci-dessous:

Quatrième étape. **Cliquez** sur 

pour afficher la fenêtre *Spybot – Rechercher des mises à jour*, et rendez-vous directement à la section **Comment actualiser les règles de détection et les bases de données de vaccination de Spybot**.

- Si vous *n'êtes pas* connecté à Internet, suivez les étapes énumérées ci-dessous:

Cinquième étape. **Cliquez** sur 

pour afficher la fenêtre *Vaccination du système*, et lancer la vaccination du système, tel qu'illustré ci-dessous:

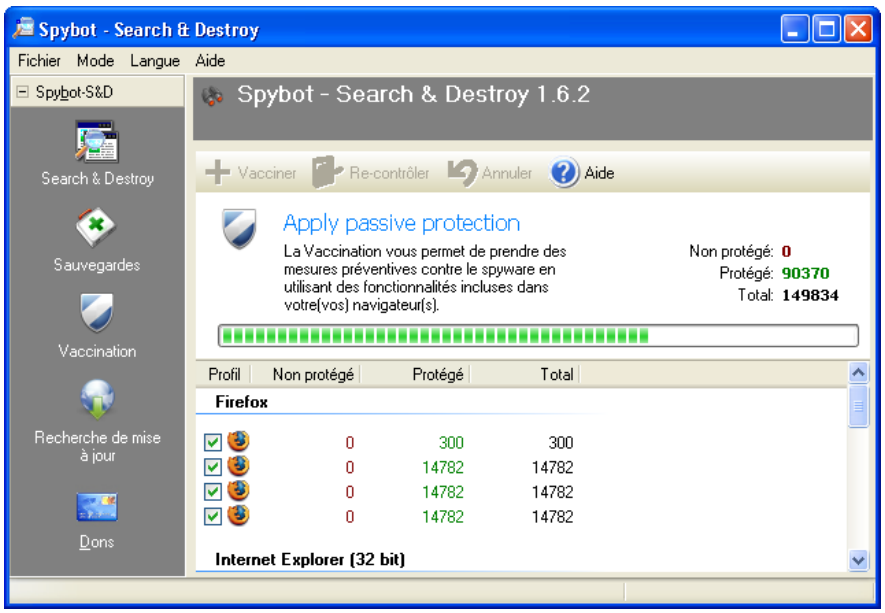
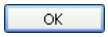


Figure 5: Le processus de vaccination en cours

Commentaire: Si vous avez laissé une page de navigateur ouverte, la fenêtre suivante s'affichera avant que le processus de vaccination se mette en marche:

Spybot - Search & Destroy
Spybot - Search & Destroy
Open browsers detected!
You should close all browsers to make sure immunization is successful.
Show list of browsers
OK
Help
Show this dialog again?

Figure 6: The Open Browser Detected screen

Sixième étape. **Fermez** votre navigateur, puis **cliquez** sur 

pour vacciner votre système.

Septième étape. **Cliquez** sur

, puis **cliquez** sur

pour revenir à la console de *Spybot - Search & Destroy* en mode *Vaccination*.

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Search & Destroy
Sauvegardes
Vaccination
Mise à jour
Dons
Spybot - Search & Destroy 1.6.0
Vérifier tout
Utilisez ce bouton pour lancer sur votre système la recherche du spyware et de toutes les autres menaces que Spybot - Search & Destroy détecte.
Sauvegardes
Utilisez ce bouton si vous avez remarqué des difficultés survenues depuis une récente correction de problèmes, et si vous voulez annuler certaines modifications.
Rechercher des mises à jou
Ceci est très important: il est conseillé de mettre à jour les détections au moins une fois par semaine!
Spybot
Search&Destroy

Figure 8: La console Spybot - Search & Destroy

2.3 Comment actualiser les règles de détection et les bases de données de vaccination de Spybot

Important: Il est crucial que vous mainteniez **Spybot** à jour avec les plus récentes définitions.

Première étape. **Cliquez** sur

dans le menu de gauche de *Spybot-S&D* pour afficher la fenêtre *Spybot-S&D Mise à jour* présentant une liste de serveurs d'où il est possible de télécharger les mises à jour.

Deuxième étape. **Choisissez** l'emplacement le plus rapproché de votre lieu de résidence, puis **cliquez à droite** et **sélectionnez** l'option *Positionner ce serveur comme miroir préféré* tel qu'illustré à la *figure 9* ci-dessous.

- Si vous avez effectué la mise à jour des règles de détection récemment, une fenêtre apparaît pour vous aviser qu'**Aucune mise à jour n'est disponible**.
- Si vous n'avez pas effectué la mise à jour des règles de détection récemment, la fenêtre de *Mises à jour de Spybot-S&D* apparaît, affichant une liste de serveurs d'où il est possible de télécharger les mises à jour ::

Spybot-S&D Mise à jour
Veuillez choisir un lieu de téléchargement des mises à jour. Les mises à jour se feront plus vite si vous choisissez un emplacement proche de vous.
Miroir
Positionner ce serveur comme miroir préféré
Effacer le paramètre de miroir préféré
BN FileForum #2
BN FileForum (G
ComputerFixerTools.com (USA)
Computer-Woerterbuch.de (Germany)
Connect plus s.r.o. (Czech Republic)
Evertje Networks (Netherlands)
FirstNetServ (Europe)
FreewareArchiv (Germany)
Gehirnbrand (Germany)
Gigenet (USA)
HTML.it (Italy)
Safer-Networking #1 (Europe)
Safer-Networking #2 (Europe)
Continuer

Figure 9: La fenêtre Spybot-S&D Mise à jour

Troisième étape. **Cliquez** sur

pour afficher la fenêtre *Spybot-S&D Mise à jour - Veuillez choisir les mises à jour à télécharger ici.*

Quatrième étape. **Cochez** toutes les options présentées, puis **cliquez** sur

pour lancer le téléchargement de ces mises à jour.

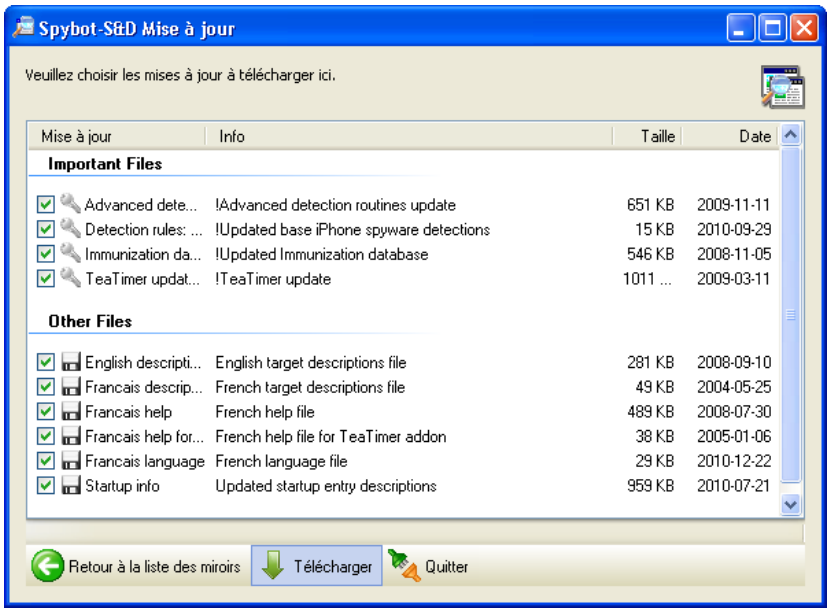

Spybot-S&D Mise à jour
Veuillez choisir les mises à jour à télécharger ici.
Mise à jour
Info
Taille
Date
Important Files
Advanced dete... !Advanced detection routines update 651 KB 2009-11-11
Detection rules: ... !Updated base iPhone spyware detections 15 KB 2010-09-29
Immunization da... !Updated Immunization database 546 KB 2008-11-05
TeaTimer updat... !TeaTimer update 1011 ... 2009-03-11
Other Files
English descripti... English target descriptions file 281 KB 2008-09-10
Francais descrip... French target descriptions file 49 KB 2004-05-25
Francais help French help file 489 KB 2008-07-30
Francais help for... French help file for TeaTimer addon 38 KB 2005-01-06
Francais language French language file 29 KB 2010-12-22
Startup info Updated startup entry descriptions 959 KB 2010-07-21
Retour à la liste des miroirs
Télécharger
Quitter

Figure 10: La fenêtre de mise à jour de Spybot-S&D affichant les règles de détection, les fichiers d'aide et les bases de données de vaccination

Commentaire: Si une erreur se produit pendant le téléchargement de ces mises à jour, Spybot vous donnera l'occasion de réessayer. Après avoir terminé le téléchargement avec succès, le programme vous invitera à vacciner votre système et à vérifier s'il comporte des problèmes:

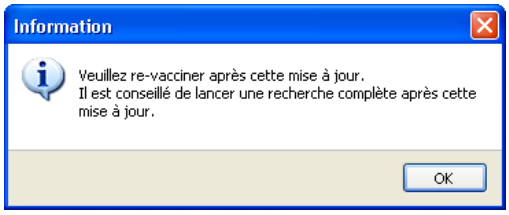
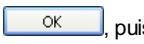

Information
Veuillez re-vacciner après cette mise à jour.
Il est conseillé de lancer une recherche complète après cette mise à jour.
OK

Figure 11: La fenêtre Information

Sixième étape. **Cliquez** sur 

, puis sur

.

Vous serez alors redirigé vers la fenêtre principale de Spybot - Search & Destroy

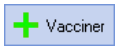
Commentaire: Vous pouvez également exécuter le processus de mise à jour de Spybot en tout temps en: **Sélectionnant : Démarrer > Programmes > Spybot Search & Destroy > Update Spybot S&D**.

2.4 Comment vacciner votre système

Spybot contribue à protéger votre ordinateur contre les logiciels malveillants et les mouchards identifiés en procédant à sa "vaccination". C'est un exercice similaire à la vaccination que nous recevons pour nous prémunir contre les maladies infectieuses.

Pour vacciner votre système informatique, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur

dans le menu **Spybot-S&D** ou 

pour automatiquement lancer le processus de vaccination, tel qu'illustré à la *figure 6* ci-dessus.

Vous devrez peut-être agrandir la fenêtre pour afficher toutes les options du panneau *Vaccination*.

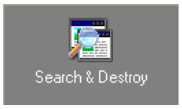
Commentaire: Il est possible de renverser ou défaire le processus de vaccination si vous craignez que la vaccination du système ait eu un effet négatif sur la performance de votre ordinateur. Vous pouvez **cliquer** sur

pour renverser le processus de vaccination et restaurer votre système à son état précédent.

2.5 Comment détecter la présence de problèmes

Rappel: Avant de commencer à vérifier votre système pour y détecter de potentielles menaces, il est important d'actualiser les *règles de détection* et les *bases de données de vaccination* de **Spybot**.

Pour contrôler la présence de problèmes et de menaces, suivez les étapes ci-dessous:

Première étape. **Cliquez** sur 

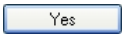
pour afficher le panneau de **Spybot** *Search and Destroy*.

Deuxième étape. **Cliquez** sur

pour entamer la vérification du système et y détecter d'éventuelles menaces (si vous avez un gros volume de données, de fichiers et de programmes, etc., cette étape peut prendre entre 20 minutes et une heure). Il est possible qu'une fenêtre d'invite comme celle-ci s'affiche:

Spybot
Search&Destroy
We have located 7722 temporary files...
Scan speed will increase if you allow us to clean your temporary folder. Dou you want Spybot-S&D to do this for you?
Yes
No (14)
Never (will not ask again)

Figure 12: Le programme Spybot - S&D vérifiant le système pour y détecter des problèmes.

Troisième étape. **Cliquez** sur 

pour entamer la vérification du système:

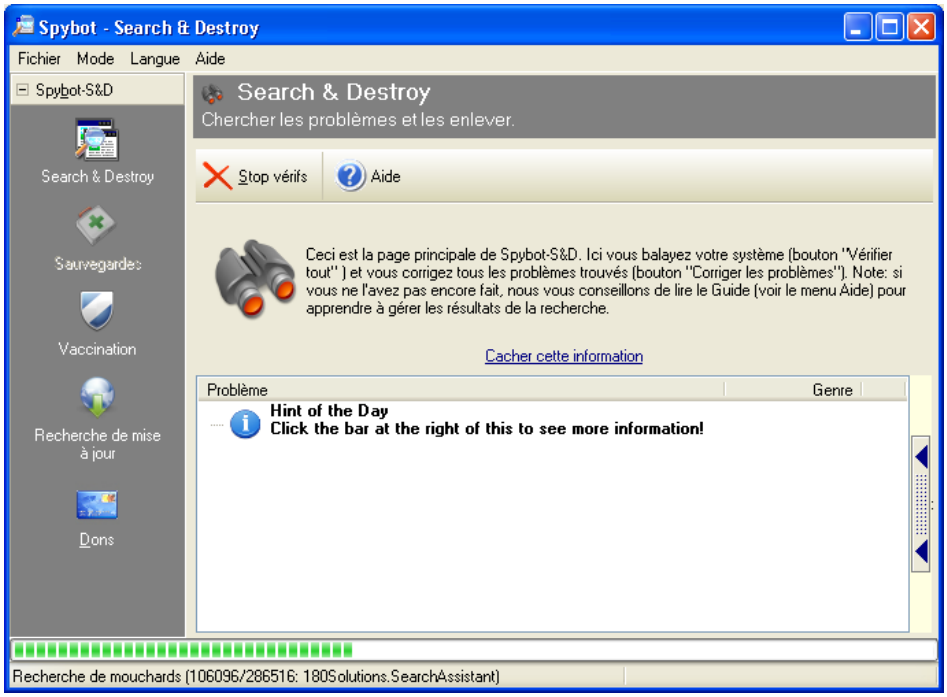

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Search & Destroy
Sauvegardes
Vaccination
Recherche de mise à jour
Dons
Search & Destroy
Chercher les problèmes et les enlever.
Stop vérifs
Aide
Ceci est la page principale de Spybot-S&D. Ici vous balayez votre système (bouton "Vérifier tout") et vous corrigez tous les problèmes trouvés (bouton "Corriger les problèmes"). Note: si vous ne l'avez pas encore fait, nous vous conseillons de lire le Guide (voir le menu Aide) pour apprendre à gérer les résultats de la recherche.
Cacher cette information
Problème
Genre
Hint of the Day
Click the bar at the right of this to see more information!
Recherche de mouchards (106096/286516: 180Solutions.SearchAssistant)

Figure 13: Le programme Spybot - S&D vérifiant le système pour y détecter des problèmes.

Lorsque la vérification est achevée, le nombre et la nature des problèmes est listée dans le panneau principal::

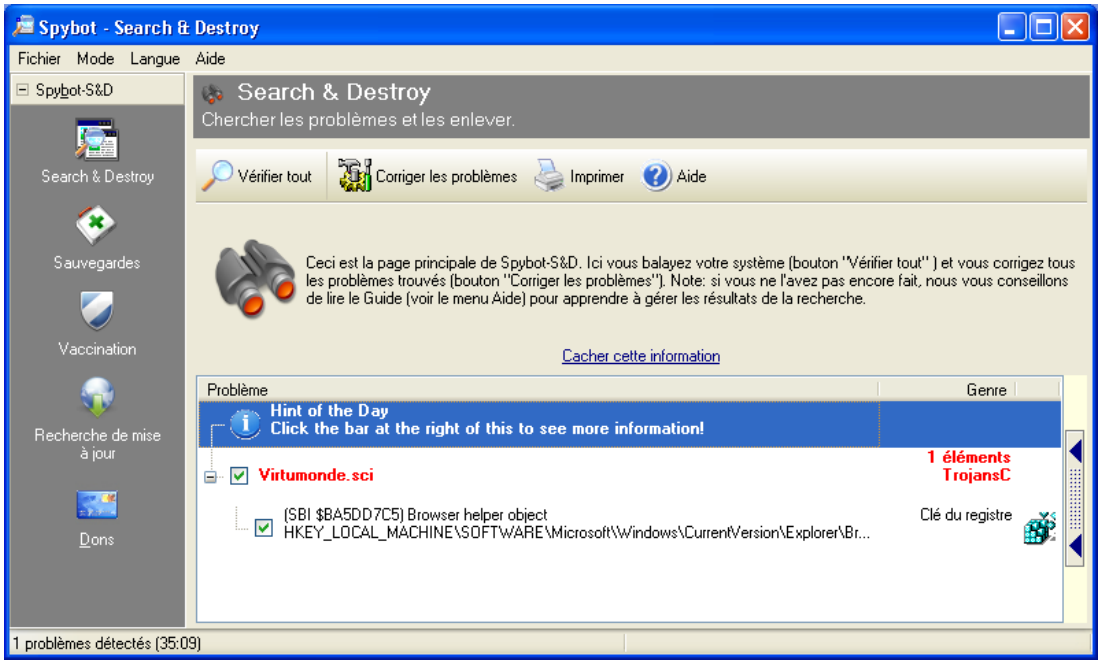

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Search & Destroy
Sauvegardes
Vaccination
Recherche de mise à jour
Dons
Search & Destroy
Chercher les problèmes et les enlever.
Vérifier tout
Corriger les problèmes
Imprimer
Aide
Ceci est la page principale de Spybot-S&D. Ici vous balayez votre système (bouton "Vérifier tout") et vous corrigez tous les problèmes trouvés (bouton "Corriger les problèmes"). Note: si vous ne l'avez pas encore fait, nous vous conseillons de lire le Guide (voir le menu Aide) pour apprendre à gérer les résultats de la recherche.
Cacher cette information
Problème
Genre
Hint of the Day
Click the bar at the right of this to see more information!
Virtumonde.sci
1 éléments
TrojansC
(SBI $BA5DD7C5) Browser helper object
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br...
Clé du registre
1 problèmes détectés (35:09)

Figure 14: La fenêtre principale de Spybot - S&D affichant les problèmes et menaces potentielles

Quatrième étape. Ne **cochez** uniquement que les éléments que vous souhaitez supprimer. Certains des éléments trouvés sont peut-être des logiciels publicitaires que vous souhaitez conserver (pour une raison ou une autre).

Astuce: Tous les éléments affichés en lettres rouges sont généralement considérés comme des problèmes ou des menaces. Tous les éléments affichés en lettres vertes servent à surveiller vos habitudes d'utilisation d'Internet. Pour conserver un élément en particulier, décocher la case qui y est associée et cet élément ne sera pas supprimé.

Important: Avant de supprimer ou ignorer un logiciel malveillant que vous avez trouvé, il est fortement recommandé d'en examiner le comportement et l'origine.

Cinquième étape. **Cliquez** sur du côté droit de la fenêtre des résultats de Spybot, pour afficher des renseignements sur l'élément trouvé. Si rien ne s'affiche, vous pouvez effectuer une recherche sur Internet. Renseignez-vous sur le fonctionnement et le comportement de l'élément trouvé et sur comment il peut compromettre l'intégrité et la sécurité de votre système. Une meilleure connaissance des problèmes et des menaces entraîne une plus grande sécurité et une meilleure protection de votre vie privée.

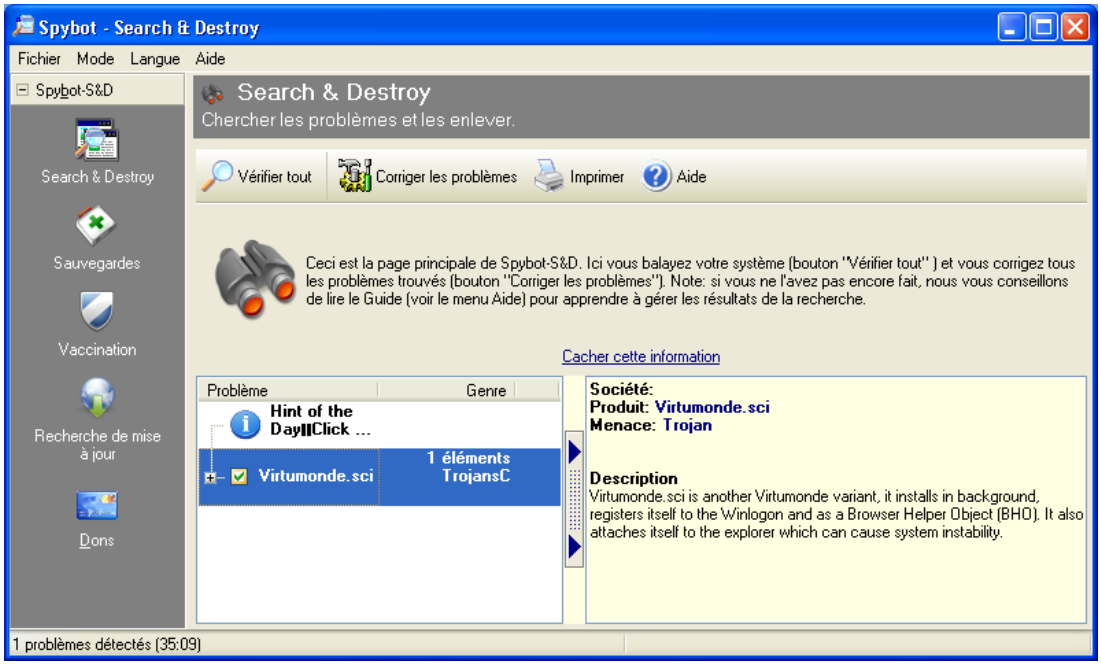
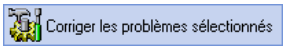

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Search & Destroy
Sauvegardes
Vaccination
Recherche de mise à jour
Dons
Search & Destroy
Chercher les problèmes et les enlever.
Vérifier tout
Corriger les problèmes
Imprimer
Aide
Ceci est la page principale de Spybot-S&D. Ici vous balayez votre système (bouton "Vérifier tout") et vous corrigez tous les problèmes trouvés (bouton "Corriger les problèmes"). Note: si vous ne l'avez pas encore fait, nous vous conseillons de lire le Guide (voir le menu Aide) pour apprendre à gérer les résultats de la recherche.
Cacher cette information
Problème
Genre
Hint of the DayClick ...
Virtumonde.sci
1 éléments
TrojansC
Société:
Produit: Virtumonde.sci
Menace: Trojan
Description
Virtumonde.sci is another Virtumonde variant, it installs in background, registers itself to the Winlogon and as a Browser Helper Object (BHO). It also attaches itself to the explorer which can cause system instability.
1 problèmes détectés (35:09)

*Figure 15: Le panneau Afficher plus d'informations de Spybot - S&D *

Sixième étape. **Cliquez** sur 

pour activer la suppression des logiciels malveillants.

Une boîte de dialogue apparaît vous demandant de confirmer que vous souhaitez supprimer tous les problèmes trouvés.

Septième étape. **Cliquez** sur le bouton *oui* si vous souhaitez les supprimer.

Commentaire: De façon générale, il est recommandé d'effectuer une vérification du système chaque semaine.

2.6 Le Résident TeaTimer

Le **Résident TeaTimer** est un programme de **Spybot** qui tourne constamment en arrière-plan (c.-à-d. même lorsque vous n'êtes pas en train d'utiliser **Spybot**). Le programme surveille continuellement les principaux processus du système pour s'assurer qu'aucune menace potentielle ne modifie les configurations ou les paramètres essentiels du système. **TeaTimer** vous alerte chaque fois qu'un processus suspect ou malveillant est détecté et vous demande d'*autoriser* ou de *refuser* ce processus (si celui-ci s'avère malveillant). Voici un exemple d'alerte de **TeaTimer** :

Figure 16: Une alerte du Résident TeaTimer de Spybot - S&D, présentant le choix d'autoriser ou de refuser le changement

Étant donné que plusieurs programmes (qu'ils soient nécessaires ou malveillants) exigent un accès aux processus internes du système, **TeaTimer** vous demandera régulièrement d'*autoriser* ou de *refuser* des changements. Dans cet exemple, **Skype** est supprimé du menu de Démarrage de Windows. Cela se produit habituellement lorsque vous désinstallez un programme (et pas nécessairement uniquement lors du démarrage). Dans ce cas, il s'agit d'une requête valide concernant une modification mineure à un paramètre du système et vous pouvez donc l'autoriser.

Astuce: Si vous n'êtes pas certain de comprendre l'alerte de **TeaTimer** et aimeriez obtenir un supplément d'information, **cliquez** sur

.

Spybot-S&D Resident - Startup entry database
Current filename: "C:\Program Files\Skype\Phone \Skype.exe" /nosplash /minimized
Database status: Typically not required
Value: Skype
Filename: Skype.exe
Description
" Skype is free and simple software that will enable you to make free calls anywhere in the world in minutes"
Source: Paul Collins Startup list
OK

Figure 17: La fenêtre de démarrage de Spybot - Search & Destroy

Il est plus sûr de refuser une requête si vous n'êtes pas certain de l'action posée. Par contre, si vous êtes certain que la requête est légitime, cocher la case *Se rappeler de cette décision* et **Spybot** n'affichera plus cette alerte à l'avenir.

Commentaire: Vous verrez souvent TeaTimer s'activer lorsque vous installez un nouveau programme et que celui-ci tente de s'ajouter au processus de démarrage. La même chose se produit lorsque vous désinstallez un programme.

Astuce: Il est fortement recommandé d'actualiser TeaTimer chaque fois que des mises à jour sont disponibles.

2.7 Comment utiliser l'outil de Sauvegardes

L'outil de *Sauvegardes* permet de récupérer ou de retrouver chaque élément précédemment supprimé ou réparé. Cela est possible car **Spybot** crée une copie de sauvegarde pour chaque élément supprimé. Si un logiciel malveillant est supprimé et que cela entraîne une défaillance de l'ordinateur, il est possible de récupérer l'élément en question en utilisant l'outil de *Sauvegardes*.

Pour récupérer un élément précédemment supprimé, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur

pour afficher la fenêtre de *Sauvegardes* illustrée ci-dessous :

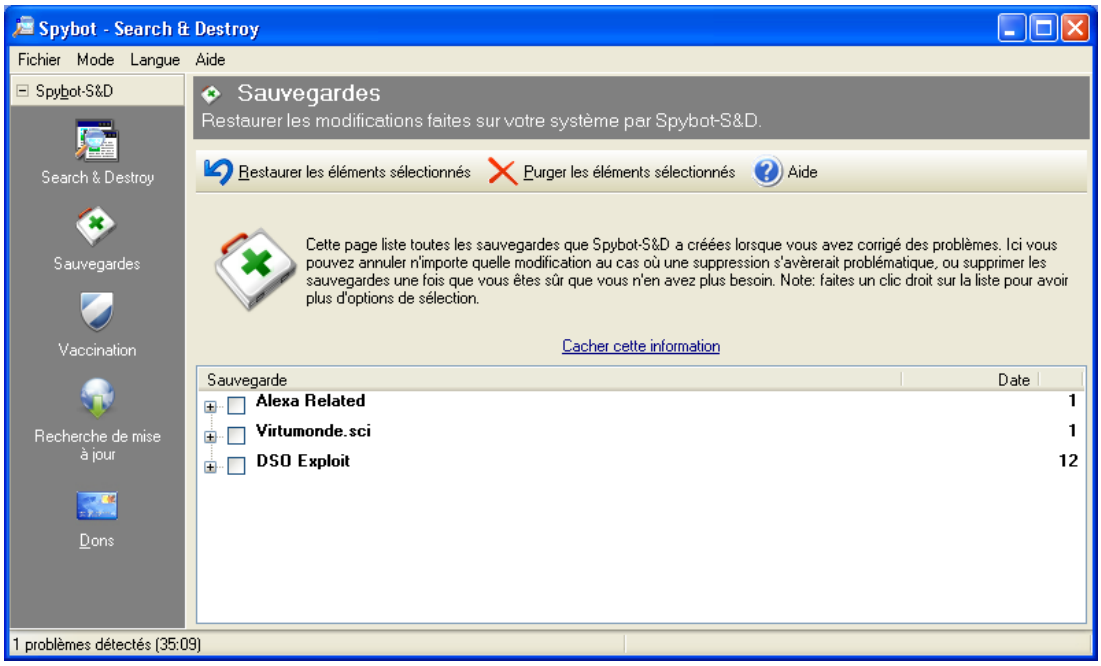

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Search & Destroy
Sauvegardes
Vaccination
Recherche de mise à jour
Dons
Sauvegardes
Restaurer les modifications faites sur votre système par Spybot-S&D.
Restaurer les éléments sélectionnés
Purger les éléments sélectionnés
Aide
Cette page liste toutes les sauvegardes que Spybot-S&D a créées lorsque vous avez corrigé des problèmes. Ici vous pouvez annuler n'importe quelle modification au cas où une suppression s'avèrerait problématique, ou supprimer les sauvegardes une fois que vous êtes sûr que vous n'en avez plus besoin. Note: faites un clic droit sur la liste pour avoir plus d'options de sélection.
Cacher cette information
Sauvegarde
Date
Alexa Related 1
Virtumonde.sci 1
DSO Exploit 12
1 problèmes détectés (35:09)

Figure 18: La fenêtre de sauvegardes de Spybot - Search & Destroy

Deuxième étape. Dans la liste des éléments précédemment supprimés, **cochez** les éléments que vous souhaitez récupérer, puis **cliquez** sur

.

Une boîte de dialogue de confirmation est alors activée:

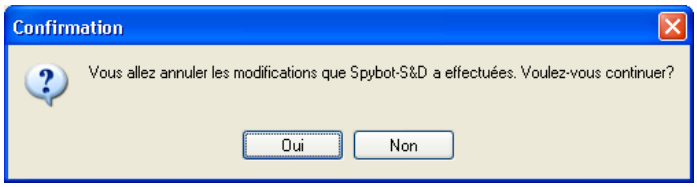


Figure 19: La boîte de dialogue de confirmation

Troisième étape. **Cliquez** sur

pour récupérer ces éléments.

Quatrième étape. Autrement, **cliquez** sur

pour éliminer définitivement les éléments cochés. Cependant, soyez conscient que les éléments purgés ne seront plus récupérables.

Comment utiliser Spybot en mode avancé

- **3.0 À propos du mode avancé**
- **3.1 Comment activer le mode avancé**
- **3.2 Comment utiliser les outils du mode avancé**

3.0 À propos du mode avancé*

Spybot fonctionne en mode *par défaut* et en mode *avancé*. Le mode *avancé* vous permet d'accéder aux paramètres du programme, ainsi qu'à des outils supplémentaires.

3.1 Comment activer le mode avancé

Pour activer le mode *avancé* de **Spybot**, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Mode > Mode avancé** dans la barre menu:

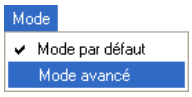


Figure 1: Les options du sous-menu Mode

Cette action activera la fenêtre suivante:

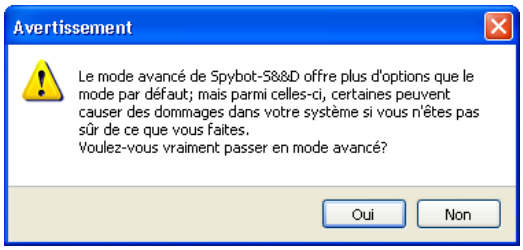

Avertissement
Le mode avancé de Spybot-S&D offre plus d'options que le mode par défaut; mais parmi celles-ci, certaines peuvent causer des dommages dans votre système si vous n'êtes pas sûr de ce que vous faites.
Voulez-vous vraiment passer en mode avancé?
Oui
Non

Figure 2: La fenêtre d'invite Avertissement

Deuxième étape. **Cliquez** sur Oui pour confirmer le choix du mode *avancé*.

Dans le mode *avancé* , le menu latéral de **Spybot** comporte plus d'options que sous le mode par défaut:

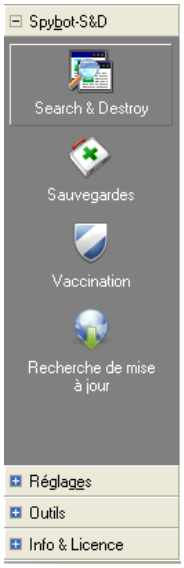


Figure 3: Le menu latéral du mode avancé de Spybot - Search & Destroy

Troisième étape. **Double-cliquez** sur *Réglages* pour afficher les descriptions de divers éléments et options dans le panneau principal:

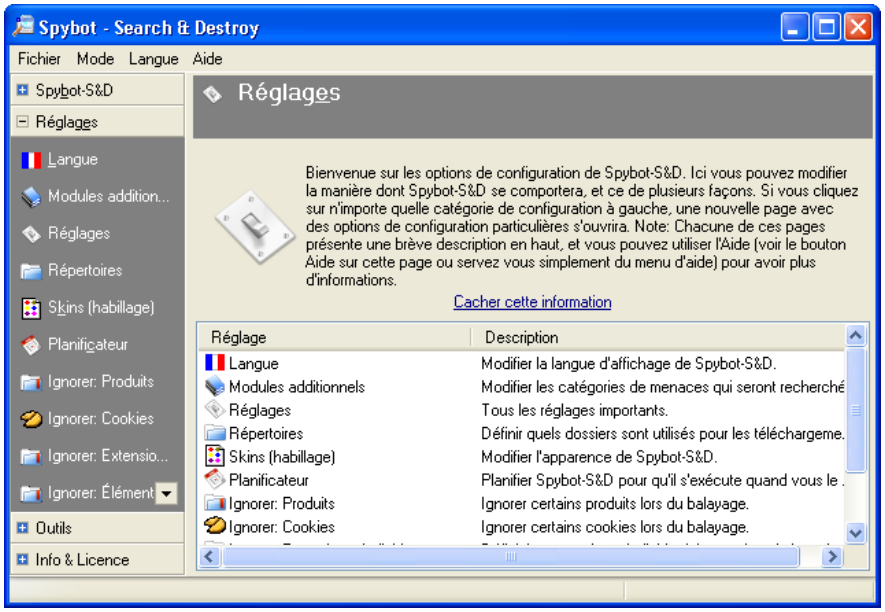

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Réglages
Langue
Modules addition...
Réglages
Répertoires
Skins (habillage)
Planificateur
Ignorer: Produits
Ignorer: Cookies
Ignorer: Extensio...
Ignorer: Élément
Outils
Info & Licence
Réglages
Bienvenue sur les options de configuration de Spybot-S&D. Ici vous pouvez modifier la manière dont Spybot-S&D se comportera, et ce de plusieurs façons. Si vous cliquez sur n'importe quelle catégorie de configuration à gauche, une nouvelle page avec des options de configuration particulières s'ouvrira. Note: Chacune de ces pages présente une brève description en haut, et vous pouvez utiliser l'Aide (voir le bouton Aide sur cette page ou servez vous simplement du menu d'aide) pour avoir plus d'informations.
Cacher cette information
Réglage
Description
Langue
Modifier la langue d'affichage de Spybot-S&D.
Modules additionnels
Modifier les catégories de menaces qui seront recherché
Réglages
Tous les réglages importants.
Répertoires
Définir quels dossiers sont utilisés pour les téléchargeme.
Skins (habillage)
Modifier l'apparence de Spybot-S&D.
Planificateur
Planifier Spybot-S&D pour qu'il s'exécute quand vous le .
Ignorer: Produits
Ignorer certains produits lors du balayage.
Ignorer: Cookies
Ignorer certains cookies lors du balayage.

Figure 4: La fenêtre réglages

Quatrième étape. **Double-cliquez** sur *outils* pour afficher les outils qui vous permettront d'identifier des mouchards que le processus de vérification normal ne suffit pas à détecter, et à refaire la vérification du système.

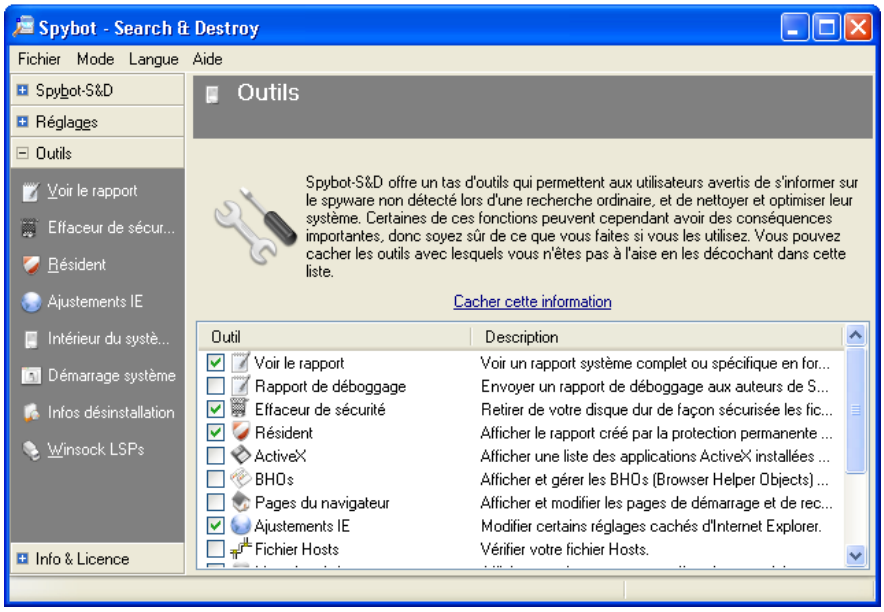

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Réglages
Outils
Voir le rapport
Effaceur de sécur...
Résident
Ajustements IE
Intérieur du systè...
Démarrage système
Infos désinstallation
Winsock LSPs
Info & Licence
Outils
Spybot-S&D offre un tas d'outils qui permettent aux utilisateurs avertis de s'informer sur le spyware non détecté lors d'une recherche ordinaire, et de nettoyer et optimiser leur système. Certaines de ces fonctions peuvent cependant avoir des conséquences importantes, donc soyez sûr de ce que vous faites si vous les utilisez. Vous pouvez cacher les outils avec lesquels vous n'êtes pas à l'aise en les décochant dans cette liste.
Cacher cette information
Outil
Description
Voir le rapport
Voir un rapport système complet ou spécifique en for...
Rapport de déboggage
Envoyer un rapport de déboggage aux auteurs de S...
Effaceur de sécurité
Retirer de votre disque dur de façon sécurisée les fic...
Résident
Afficher le rapport créé par la protection permanente ...
ActiveX
Afficher une liste des applications ActiveX installées ...
BHOs
Afficher et gérer les BHOs (Browser Helper Objects) ...
Pages du navigateur
Afficher et modifier les pages de démarrage et de rec...
Ajustements IE
Modifier certains réglages cachés d'Internet Explorer.
Fichier Hosts
Vérifier votre fichier Hosts.

Figure 5: La fenêtre outils

Cinquième étape. **Double-cliquez** sur *Info & Licence* pour afficher les renseignements généraux et l'information portant sur la licence d'utilisation de **Spybot 1.6.2**.

3.2 Comment utiliser les outils du mode avancé

Les utilisateurs **avancés** apprécieront les options avancées offertes par **Spybot**: *Ajustements IE* , *Effaceur de sécurité*, *Intérieur du système* et *Démarrage système*.

3.2.1 Ajustements IE

L'option *Ajustements IE* sert à la configuration d'**Internet Explorer**. Cela vous permet de configurer certains paramètres de sécurité importants d'IE, en particulier lorsque plusieurs utilisateurs se servent d'un même système.

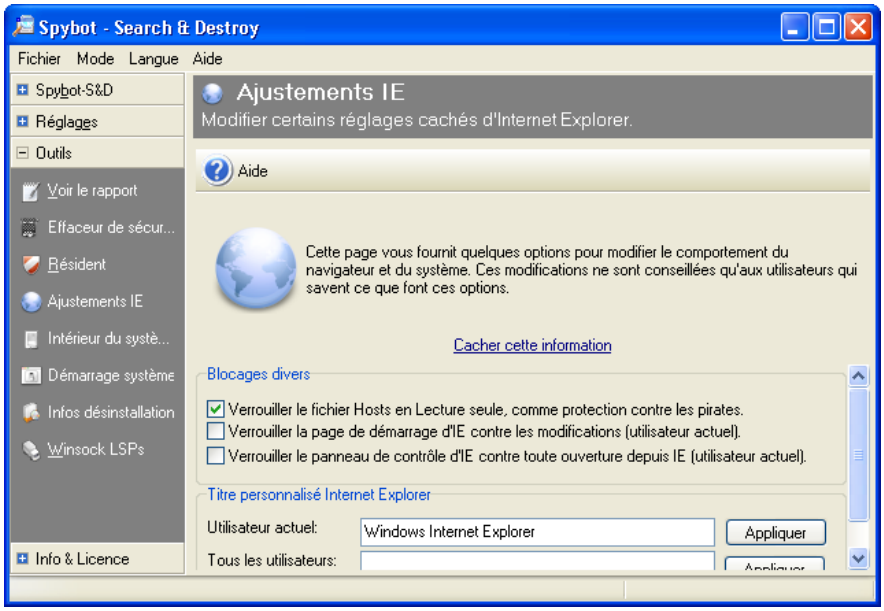

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Réglages
Outils
Voir le rapport
Effaceur de sécur...
Résident
Ajustements IE
Intérieur du systè...
Démarrage système
Infos désinstallation
Winsock LSPs
Info & Licence
Ajustements IE
Modifier certains réglages cachés d'Internet Explorer.
Aide
Cette page vous fournit quelques options pour modifier le comportement du navigateur et du système. Ces modifications ne sont conseillées qu'aux utilisateurs qui savent ce que font ces options.
Cacher cette information
Blocages divers
Verrouiller le fichier Hosts en Lecture seule, comme protection contre les pirates.
Verrouiller la page de démarrage d'IE contre les modifications (utilisateur actuel).
Verrouiller le panneau de contrôle d'IE contre toute ouverture depuis IE (utilisateur actuel).
Titre personnalisé Internet Explorer
Utilisateur actuel:
Windows Internet Explorer
Appliquer
Tous les utilisateurs:

Figure 6: La fenêtre Ajustements IE

Vous devriez toujours laisser la première option cochée, tel qu'illustré dans l'exemple ci-dessus.

3.2.2 Effaceur de sécurité

Voici une option très pratique pour supprimer définitivement (effacer) des fichiers temporaires de **Windows** et du navigateur Internet. Pour plus d'information sur la suppression définitive de fichiers temporaires, consultez le chapitre **6. Détruire définitivement des données sensibles** [37] du livret pratique Security in-a-Box.

Première étape. **Cliquez** sur

pour afficher la fenêtre suivante:

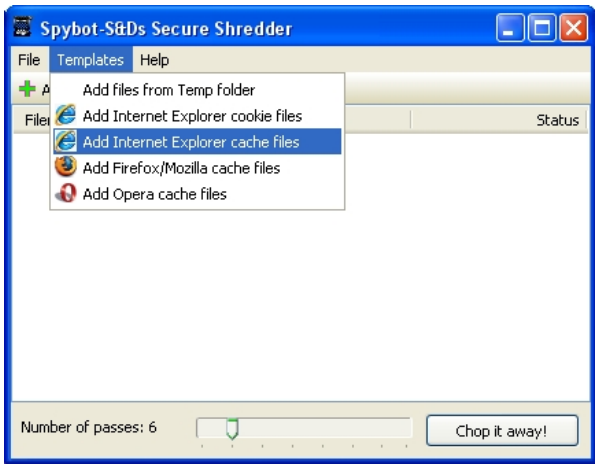


Figure 7: La fenêtre de l'Effaceur de sécurité de Spybot-S&D

Deuxième étape. **Cliquez** sur *Templates* pour activer un menu défilant des emplacements où se trouvent des fichiers temporaires, tel qu'illustré à la *figure 7*, puis **sélectionnez** un item dans la liste pour remplir la fenêtre de l'*Effaceur de sécurité de Spybot-S&D*:

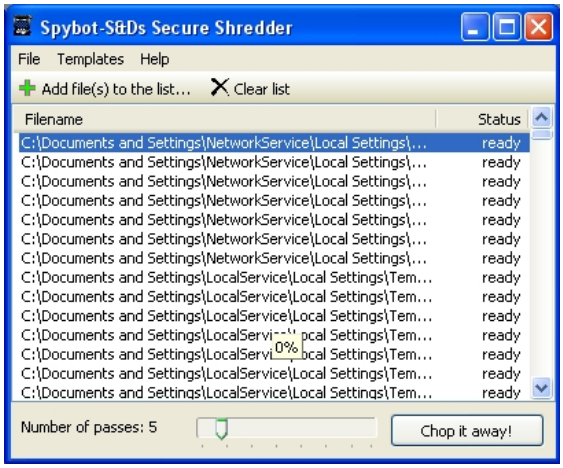
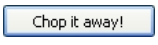


Figure 8: La liste des fichiers temporaires dans la fenêtre de l'Effaceur de sécurité

Troisième étape. **Sélectionnez** un ou des fichier(s) à supprimer.

Quatrième étape*. **Déterminer le nombre de passages utilisés pour effacer le(s) fichier(s) sélectionné(s):

Figure 9: Choisissez le nombre de passages désiré

Cin quième étape. **Cliquez** sur 

après avoir déterminé le nombre de passages que comptera la processus de suppression

***Spybot** supprimera définitivement de votre ordinateur tous les fichiers temporaires non nécessaires.*

Vous pouvez également utiliser l'*Effaceur de sécurité* pour supprimer et effacer d'autres fichiers. Pour ce faire, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez > Add file(s) to the list...** pour afficher la fenêtre suivante:

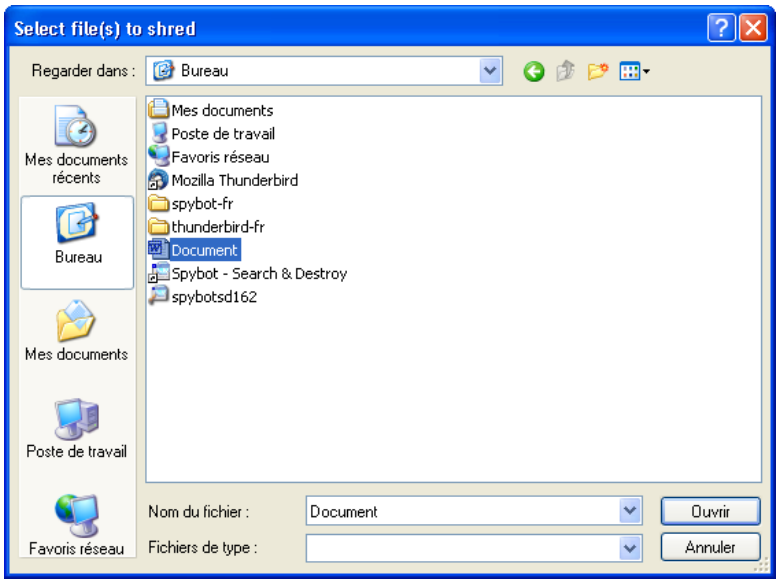


Figure 10: La fenêtre de navigateur Select File(s) to shred

Deuxième étape. **Sélectionnez** le fichier que vous souhaitez effacer.

Troisième étape. **Cliquez** sur

pour afficher le fichier dans la *figure 8*, puis **cliquez** ![] sur (/sbox/screen/spybot-fr/61.png) pour supprimer et effacer le fichier.

3.2.3 Intérieur du système (Pour utilisateurs avancés seulement!)

L'outil *Intérieur du système* cherchera des fichiers incorrectement nommés ou dotés de noms incohérents dans le **Registre Windows**. L'explication détaillée du registre de Windows est donnée dans le Guide pratique **CCleaner** [36].

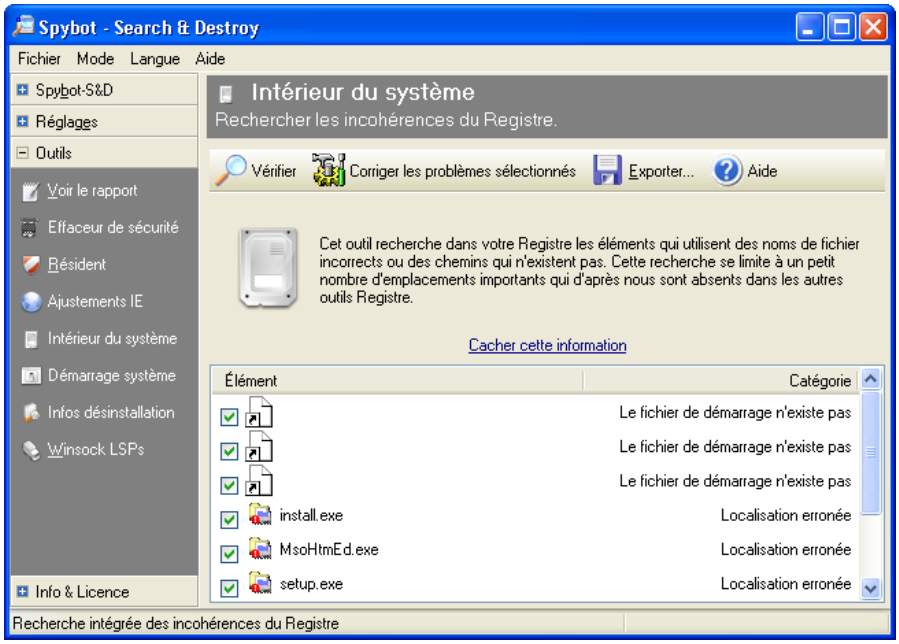
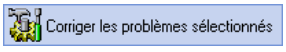


Figure 11: La fenêtre Intérieur du système

Première étape. **Cliquez** sur

pour entamer la recherche de problèmes dans le **Registre Windows**.

Deuxième étape. Lorsque la vérification est terminée, **cliquez** sur 

pour corriger tous les problèmes trouvés.

3.2.4 Démarrage système (Pour utilisateurs avancés seulement!)

L'outil *Démarrage système* affiche, en ordre séquentiel, tous les programmes chargés par **Windows** au démarrage de l'ordinateur. Il vous laisse départager ceux qui sont nécessaires de ceux qui ne sont pas essentiels au démarrage.

Astuce: Le retrait de certains éléments de cette liste augmente la vitesse à laquelle **Windows** démarre.

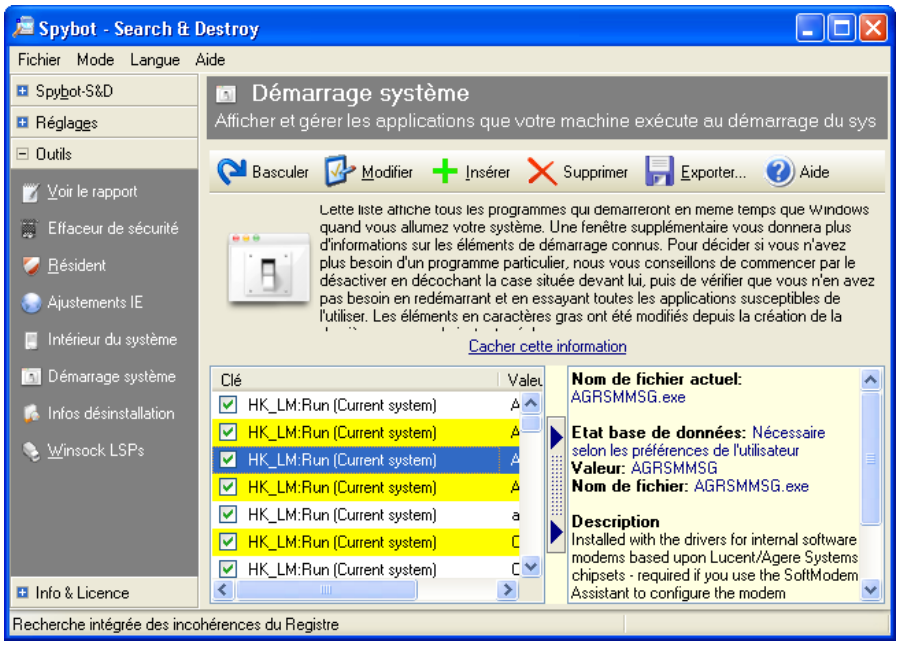

Spybot - Search & Destroy
Fichier Mode Langue Aide
Spybot-S&D
Réglages
Outils
Voir le rapport
Effaceur de sécurité
Résident
Ajustements IE
Intérieur du système
Démarrage système
Infos désinstallation
Winsock LSPs
Info & Licence
Démarrage système
Afficher et gérer les applications que votre machine exécute au démarrage du sys
Basculer
Modifier
Insérer
Supprimer
Exporter...
Aide
Cette liste affiche tous les programmes qui demarreront en meme temps que Windows quand vous allumez votre système. Une fenêtre supplémentaire vous donnera plus d'informations sur les éléments de démarrage connus. Pour décider si vous n'avez plus besoin d'un programme particulier, nous vous conseillons de commencer par le désactiver en décochant la case située devant lui, puis de vérifier que vous n'en avez pas besoin en redémarrant et en essayant toutes les applications susceptibles de l'utiliser. Les éléments en caractères gras ont été modifiés depuis la création de la
Cacher cette information
Clé
Valeu
HK_LM:Run (Current system)
Nom de fichier actuel:
AGRSMMSG.exe
Etat base de données: Nécessaire
selon les préférences de l'utilisateur
Valeur: AGRSMMSG
Nom de fichier: AGRSMMSG.exe
Description
Installed with the drivers for internal software modems based upon Lucent/Agere Systems chipsets - required if you use the SoftModem Assistant to configure the modem
Recherche intégrée des incohérences du Registre

Figure 12: La fenêtre de l'outil Démarrage système

Première étape. **Cliquez** sur pour afficher le panneau d'information.

Dans ce panneau d'information, chaque élément surligné comporte une description de son comportement et de sa fonction. Lisez attentivement ces descriptions avant de décider si oui ou non un élément doit être chargé au démarrage de **Windows**.

Faq et questions récapitulatives

4.0 Faq et questions récapitulatives

Elena et Nikolai ont tous deux l'impression que Spybot est un programme complet et facile à utiliser. Sa fonction essentielle, soit de protéger un ordinateur des infections et des mouchards, est exécutée automatiquement. Même s'ils sont un peux nerveux d'autoriser ou de refuser certains changements lorsque **TeaTimmer** sollicite leur attention, ils ont le sentiment qu'ils apprendront rapidement à différencier les processus légitimes des processus malveillants.

Q: *Si je désinstalle le programme, qu'advient-il des programmes espions que **Spybot** a trouvé lors des recherches effectuées dans le passé? Demeurent-ils "en quarantaine" sur mon ordinateur, ou sont-ils en fait supprimés?*

A: *Lorsque tu désinstalles **Spybot**, tous les éléments placés en quarantaine sont supprimés.*

Q: *Nikolai, je perd souvent la trace de cookies et de trackers dont j'ai besoin ou que je trouve utiles. Comment puis-je empêcher qu'ils soient supprimés ou réparés?*

A: *Ne t'en fais pas. Il y a plusieurs façons de protéger tes cookies utiles. Premièrement, lorsque **Spybot** a achevé la vérification du système, il dresse une liste de tous les problèmes et de toutes les menaces détectés. **Clique** sur chacun des éléments pour obtenir des renseignements supplémentaires à leur sujet et pour t'aider à décider si tu souhaites bel et bien le supprimer, ou au contraire le garder. Sinon, lance **Spybot** et **sélectionne Mode > mode avancé > Réglages**. Là, tu peux préciser quels sont les éléments ou les types d'éléments que tu souhaites exclure des missions de recherche et de destruction.*

Q: *Est-il facile de désinstaller **Spybot**?*

A: *En fait, c'est assez simple. Tu n'as qu'à **sélectionner > Démarrer> Programmes > Spybot – Search & Destroy > Uninstall Spybot S&D.***

Q: *Ma connexion Internet est plutôt lente. Comment puis-je optimiser la vitesse de téléchargement des mises à jour des règles de détection et des bases de données de vaccination?*

A: *Assure-toi de sélectionner les mises à jour qui correspondent à la région du monde où tu te trouves. Il n'y a aucune raison pour télécharger des mises à jour depuis un serveur qui se trouve en Asie si tu es toi-même quelque part en Europe, d'autant plus si tu dois économiser la bande passante. Les régions sont clairement indiquées par des petits drapeaux, tu devrais facilement pouvoir trouver un serveur près de chez-toi.

Q: *Pourquoi **Spybot** n'effectue-t-il pas des mises à jour automatiques des règles de détection et des bases de données de vaccination, directement au démarrage du programme?*

A: *Les mises à jour sont automatiques avec les versions réseau et professionnelle de **Spybot**. Puisque tu utilises une version gratuite, certaines fonctionnalités ne sont pas offertes. De toute façon, la mise à jour manuelle des règles de détection et des bases de données de vaccination de **Spybot** est relativement simple et facile. Voici une animation Flash pratique qui montre comment procéder à la mise à jour manuelle du système : **www.safer-networking.org** [38].*

4.1 Questions récapitulatives

- Qu'est-ce qu'un logiciel malveillant et comment un tel logiciel peut-il affecter mon ordinateur?
- Quel est l'utilité de **TeaTimer**?
- Lorsqu'on supprime un élément avec **Spybot**, est-il possible de le récupérer par la suite?
- À part chercher et détruire des logiciels malveillants, quelles sont les autres fonctions de **Spybot**?

Comodo - pare-feu

Short Description:

COMODO Firewall est un logiciel pare-feu bien connu et réputé. Il est gratuit pour utilisation personnelle. Ce logiciel protège votre ordinateur des connexions non autorisées depuis, et vers, l'Internet. Ce chapitre est conçu pour répondre aussi bien aux besoins des **débutants** qu'à ceux des utilisateurs **avancés**.

Online Installation Instructions:

Pour installer COMODO Firewall

- *Lisez la courte introduction aux **Guides pratiques** [1]*
- ***Cliquez** sur l'icone de **COMODO Firewall** ci-dessous pour ouvrir la page de téléchargement **personalfirewall.comodo.com/free-download.html**.*
- ***Cliquez** sur le bouton 'Click to download' dans la section 'Download Comodo Firewall for Windows'.*
- ***Cliquez** sur 'Enregistrer le fichier' pour sauvegarder le fichier 'cfw_installer_x86.exe' sur votre ordinateur, puis **double-cliquez** sur 'cfw_installer_x86.exe' pour lancer l'installation du programme.*
- *Lisez attentivement la section **2.0 Comment installer COMODO Firewall** avant de continuer.*
- *Après avoir complété l'installation de **COMODO Firewall** vous pouvez supprimer l'exécutable d'installation de votre ordinateur.*

COMODO:
[39]

Site Internet

www.personalfirewall.comodo.com [40]

Configuration requise

- Windows 2000/XP/2003/Vista
- Les privilèges d'administration sont nécessaires à l'installation

Version utilisée pour rédiger ce guide

- 5.0.16

Licence

- Gratuiciel

Lecture préalable:

- Livret pratique Security-in-a-Box chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** [4]

Niveau: 1: Débutant, 2: Moyen, **3: Intermédiaire, 4: Expérimenté**, 5: Avancé

Temps d'apprentissage: 60 minutes

Ce que vous apportera l'utilisation de cet outil:

- Une protection efficace de votre ordinateur et de votre réseau contre les attaques de tiers hostiles ou de pirates, et contre les programmes malveillants, les virus et autres menaces à vos logiciels et à votre système;
- La capacité, au moyen d'une interface de logiciel aisément configurable, de filtrer toutes les requêtes effectuées par les programmes installés sur votre ordinateur lorsque vous accédez à Internet.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

GNU/Linux comporte un pare-feu intégré (**netfilter/iptables** [41]) et présente d'excellents paramètres de sécurité. Il existe plusieurs interfaces utilisateurs simplifiées, dont **GUFW** [42] (**Graphical Uncomplicated Firewall**) (voir **plus d'information** [43]).

Mac OS contient également un puissant pare-feu intégré, qui peut être amélioré par un assortiment de modules complémentaires, dont: **NoobProof** [44] ou **IPSecuritas** [45]. Pour les utilisateurs qui en ont les moyens, nous recommandons l'achat de **Little Snitch** [46], qui permet de pousser au niveau supérieur votre sécurité et la protection de votre identité sur Internet.

À part **COMODO Firewall**, il existe de nombreuses options pour **Microsoft Windows**. Les utilisateurs pourront apprécier **ZoneAlarm Free Firewall** [47] ou **Outpost Firewall Free** [48].

1.1 À propos de cet outil

Un pare-feu agit comme un portier ou un gardien de votre ordinateur. Le pare-feu applique une série de règles quant à l'information qui doit être autorisée à accéder à votre ordinateur et celle qui doit pouvoir en sortir. Votre pare-feu est le premier programme à recevoir et à analyser l'information provenant d'Internet, et le dernier programme à balayer l'information sortante.

Le pare-feu permet d'empêcher les pirates ou d'autres intrus d'accéder aux renseignements personnels stockés sur votre ordinateur. Le programme empêche aussi les programmes malveillants d'envoyer de l'information vers Internet sans votre autorisation. **COMODO Firewall** est un logiciel pare-feu bien connu et réputé. C'est un logiciel d'exploitation libre, ce qui signifie que vous n'avez pas besoin d'obtenir une licence d'utilisation pour vous en servir.

L'utilisation d'un programme pare-feu personnalisé exige, dans les premiers temps, un investissement important de temps et d'effort. Vous devez vous assurer que tous les paramètres sont correctement réglés et adaptés à l'usage que vous faites de votre ordinateur. Une fois la période initiale d'apprentissage complétée, le pare-feu n'exigera que des interventions mineures de votre part.

Avertissement!: N'accédez jamais à Internet si aucun pare-feu n'est installé sur votre ordinateur! Même si votre modem Internet ou votre routeur possèdent leur propre pare-feu, il est fortement recommandé que vous en installiez également un sur votre ordinateur.

Comment installer Comodo Firewall

Sommaire des sections de cette page:

- **2.0 Survol du processus d'installation de COMODO Firewall**
- **2.1 Comment désactiver le pare-feu Windows**
- **2.2 COmment installer COMODO Firewall**

2.0 Survol du processus d'installation de COMODO Firewall

L'installation de **COMODO Firewall** est relativement simple et rapide. Elle comporte deux étapes: il faut dans un premier temps désactiver manuellement le pare-feu de Windows, et ensuite installer le logiciel **COMODO Firewall**.

Idéalement, vous ne devriez utiliser qu'un seul logiciel pare-feu sur votre ordinateur, en tout temps. Si vous utilisez actuellement un autre pare-feu sur votre ordinateur, vous devez le désinstaller avant d'installer **Comodo Firewall**, afin d'éviter les conflits possibles entre logiciels d'un même type.

2.1 Comment désactiver le pare-feu Windows

Pour désactiver le programme **Pare-feu Windows**, suivez les étapes énumérées ci-dessous:

Première étape: **Sélectionnez Démarrer> Panneau de configuration > Pare-feu Windows** pour afficher la fenêtre **Pare-feu Windows **.

Deuxième étape. **Cochez** l'option *Désactivé (non recommandé)* pour désactiver le **Pare-feu Windows** tel qu'illustré ci-dessous:

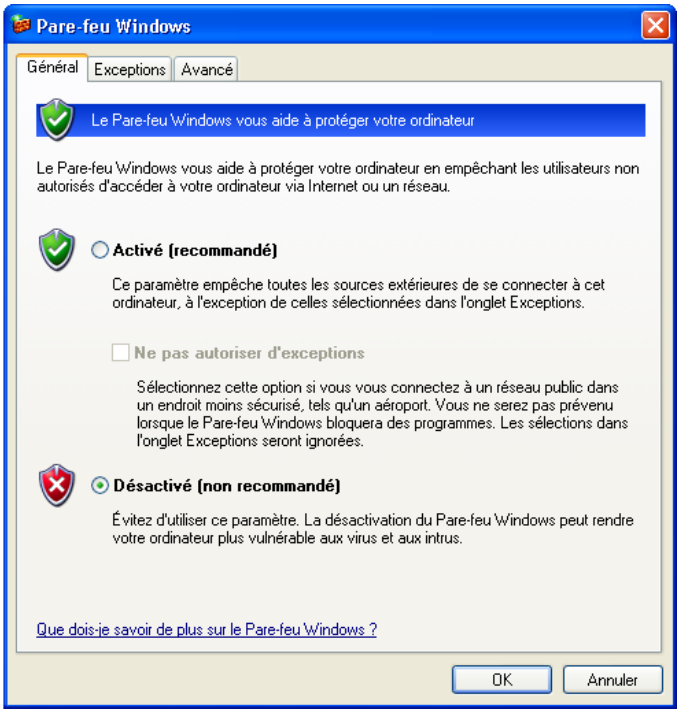

Pare-feu Windows
Général
Exceptions
Avancé
Le Pare-feu Windows vous aide à protéger votre ordinateur
Le Pare-feu Windows vous aide à protéger votre ordinateur en empêchant les utilisateurs non autorisés d'accéder à votre ordinateur via Internet ou un réseau.
Activé (recommandé)
Ce paramètre empêche toutes les sources extérieures de se connecter à cet ordinateur, à l'exception de celles sélectionnées dans l'onglet Exceptions.
Ne pas autoriser d'exceptions
Sélectionnez cette option si vous vous connectez à un réseau public dans un endroit moins sécurisé, tels qu'un aéroport. Vous ne serez pas prévenu lorsque le Pare-feu Windows bloquera des programmes. Les sélections dans l'onglet Exceptions seront ignorées.
Désactivé (non recommandé)
Évitez d'utiliser ce paramètre. La désactivation du Pare-feu Windows peut rendre votre ordinateur plus vulnérable aux virus et aux intrus.
Que dois-je savoir de plus sur le Pare-feu Windows ?
OK
Annuler

Figure 1. Le Pare-feu Windows avec l'option 'Désactivé' sélectionnée

Troisième étape. **Cliquez** sur OK pour finaliser la désactivation du *Pare-feu Windows*.

2.2 Comment installer COMODO Firewall

Commentaire: **COMODO Firewall** ne désinstalle pas automatiquement les versions plus anciennes de son logiciel. Celles-ci doivent être désinstallée manuellement avant d'entamer le processus d'installation de la plus récente version.

Pour lancer l'installation de **COMODO Firewall**, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** sur cfw_installer_x86 pour entamer le processus d'installation. Si une boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, **cliquez** sur Exécuter pour afficher la boîte de dialogue suivante:

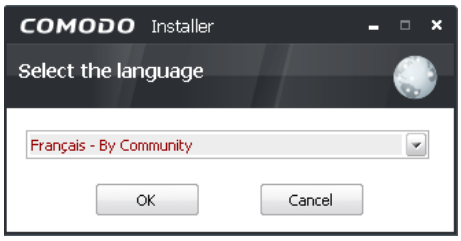


Figure 2: La boîte de dialogue de sélection de la langue

Deuxième étape. **Cliquez** sur OK pour afficher le *Contrat de licence de l'utilisateur*. Veuillez lire attentivement le *Contrat de licence de l'utilisateur* avant de poursuivre le processus d'installation du logiciel, puis **cliquez** sur J'accepte pour afficher la fenêtre *Enregistrement gratuit*.

Troisième étape: **Ne saisissez pas** votre adresse email dans le champs *Entrez votre adresse email (facultatif)*; **cliquez** simplement sur Suivant > pour afficher la fenêtre d'extraction des fichiers.

Lorsque le processus d'extraction est complété, la fenêtre *Dossier de destination* s'affiche.

Quatrième étape. **Cliquez** sur Suivant > pour accepter l'emplacement par défaut et afficher la fenêtre *Sélection du niveau de sécurité du pare-feu*, puis **cochez** l'option *Pare-feu seulement*, tel qu'illustré ci-dessous:

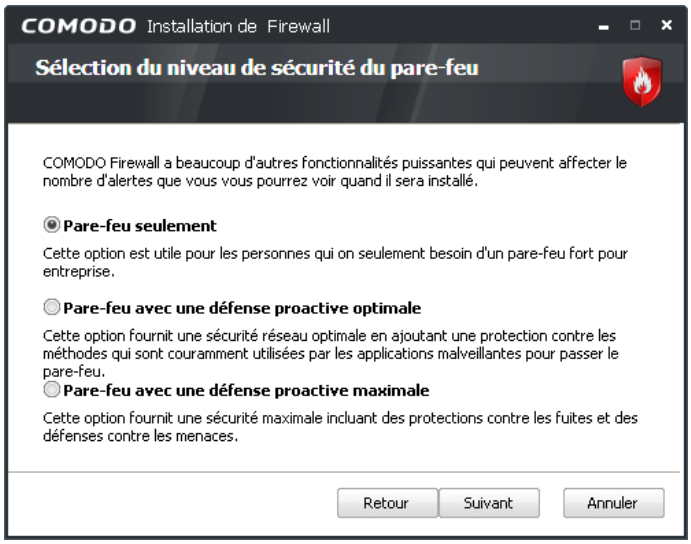

COMODO Installation de Firewall
Sélection du niveau de sécurité du pare-feu
COMODO Firewall a beaucoup d'autres fonctionnalités puissantes qui peuvent affecter le nombre d'alertes que vous vous pourrez voir quand il sera installé.
Pare-feu seulement
Cette option est utile pour les personnes qui on seulement besoin d'un pare-feu fort pour entreprise.
Pare-feu avec une défense proactive optimale
Cette option fournit une sécurité réseau optimale en ajoutant une protection contre les méthodes qui sont couramment utilisées par les applications malveillantes pour passer le pare-feu.
Pare-feu avec une défense proactive maximale
Cette option fournit une sécurité maximale incluant des protections contre les fuites et des défenses contre les menaces.
Retour
Suivant
Annuler

Figure 3: La fenêtre Sélection du niveau de sécurité du pare-feu

Définition des différents niveau de sécurité du pare-feu

Chaque niveau de sécurité du pare-feu répond aux besoins particuliers d'utilisateurs de différents niveaux. Chaque option équilibre différents types de protection selon la complexité de l'utilisation et détermine le nombre d'avertissements de sécurité que vous pourriez recevoir. Voici une brève description de chaque niveau de sécurité:

Le mode **Pare-feu seulement**: Ce mode vous permet d'utiliser **COMODO Firewall** sans la fonction *Defense +*. Le logiciel identifie les applications les plus couramment utilisées et qui sont relativement sûres (comme les navigateurs Web et les clients de courrier électronique), ce qui réduit le nombre d'avertissements de sécurité que vous pourriez recevoir. Dans ce mode, le programme explique en termes généraux pourquoi un avertissement en particulier s'affiche dans telle ou telle circonstance. De plus, les actions à entreprendre sont relativement simples.

Le mode **Pare-feu avec une défense proactive optimale**: Ce mode ajoute la fonction *Defense +* à la bonne protection de base du mode **Pare-feu seulement**. *Defense +* offre une protection active contre les logiciels malveillants conçus spécifiquement pour contourner différents pare-feu. Les *Avertissements Comodo Firewall* présentent des explications approfondies des raisons pour lesquelles certaines applications ou requêtes sont bloquées, et vous donnent l'option d'isoler des fichiers ou programmes suspects ou de les placer dans une 'sandbox'.

Le mode **Pare-feu avec une défense proactive maximale**: Ce mode combine l'option **Pare-feu avec une défense proactive optimale** avec une fonction de protection 'anti-fuite' contre les menaces 'passives', par exemple lorsque des renseignements concernant les ports ouverts sur votre ordinateur sont envoyés sur Internet. La fonction 'sandbox' est complètement automatique.

Sixième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Configuration de COMODO Secure DNS*, avec l'option *Je veux utiliser les serveurs COMODO SecureDNS* sélectionnée, tel qu'illustré ci-dessous:

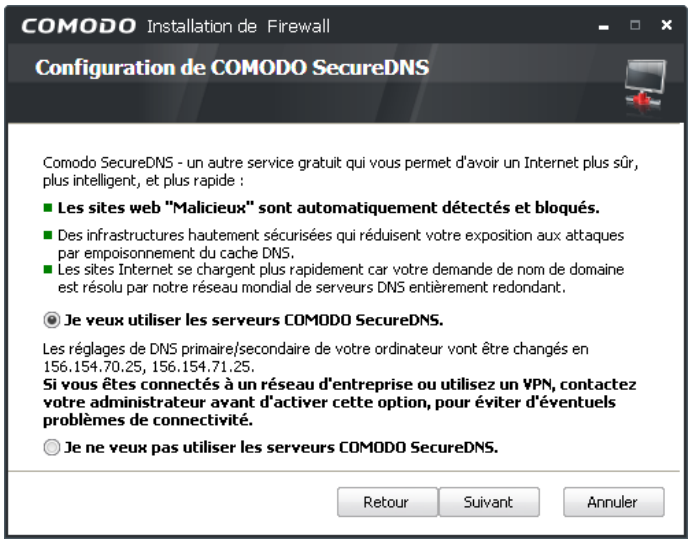

COMODO Installation de Firewall
Configuration de COMODO SecureDNS
Comodo SecureDNS - un autre service gratuit qui vous permet d'avoir un Internet plus sûr, plus intelligent, et plus rapide :
Les sites web "Malicieux" sont automatiquement détectés et bloqués.
Des infrastructures hautement sécurisées qui réduisent votre exposition aux attaques par empoisonnement du cache DNS.
Les sites Internet se chargent plus rapidement car votre demande de nom de domaine est résolu par notre réseau mondial de serveurs DNS entièrement redondant.
Je veux utiliser les serveurs COMODO SecureDNS.
Les réglages de DNS primaire/secondaire de votre ordinateur vont être changés en 156.154.70.25, 156.154.71.25.
Si vous êtes connectés à un réseau d'entreprise ou utilisez un VPN, contactez votre administrateur avant d'activer cette option, pour éviter d'éventuels problèmes de connectivité.
Je ne veux pas utiliser les serveurs COMODO SecureDNS.
Retour
Suivant
Annuler

Figure 4: La fenêtre Configuration de COMODO Secure DNS

Important: Même si aucun **Système de noms de domaine** (**DNS**) n'est parfaitement sécurisé les bénéfices liés à l'utilisation des ** Serveurs COMODO Secure DNS** sont plus nombreux que les inconvénients. Cette fonction vous offre une protection supplémentaire contre le *dévoiement (pharming)* et l'*hammeçonnage (phishing)*, deux techniques de piratage courantes employées par des tiers malveillants pour détourner votre ordinateur vers des sites hostiles ou dangereux. Facile à configurer à l'installation, la fonction **serveurs COMODO Secure DNS** peut également vous protéger des interférences du gouvernement et facilite l'accès sécurisé aux sites Internet qui sont inscrits auprès de **COMODO**. Par exemple, si vous faites une faute en saisissant une URL, vous recevrez un avertissement du **Serveur COMODO Secure DNS** semblable à celui-ci:

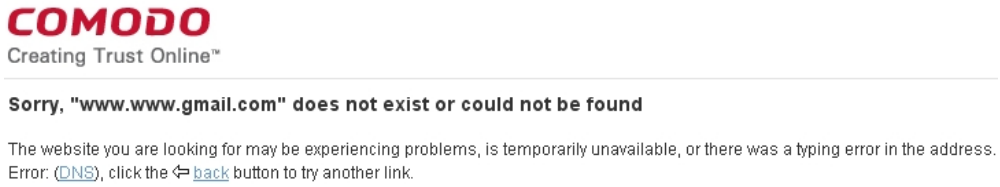

COMODO
Creating Trust Online™
Sorry, "www.www.gmail.com" does not exist or could not be found
The website you are looking for may be experiencing problems, is temporarily unavailable, or there was a typing error in the address.
Error: (DNS), click the back button to try another link.

Figure 5: Un exemple typique d'avertissement du Serveur COMODO Secure DNS

Septième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Prêt à installer COMODO Firewall*, puis **cliquez** sur Installer pour lancer l'installation et afficher la fenêtre

Installation de COMODO Firewall en cours. À l'issue du processus d'installation, la fenêtre *L'installation du COMODO Firewall est terminée* s'affiche.

Huitième étape. **Cliquez** sur Terminer pour afficher la fenêtre de confirmation *Fait*, puis **cliquez** à nouveau sur Terminer pour afficher la fenêtre de confirmation illustrée ci-dessous:

COMODO Installation de Firewall
Vous devez redémarrer votre ordinateur pour que les changement de configuration prennent effet. Cliquez sur « Oui » pour redémarrer maintenant ou « Non » si vous avez prévu de redémarrer plus tard.
Oui
Non

Figure 6: La fenêtre de confirmation Installation de Firewall

Neuvième étape. **Cliquez** sur Oui pour redémarrer l'ordinateur et finaliser la procédure d'installation de **COMODO Firewall**.

Après avoir redémarré votre ordinateur, la fenêtre *Nouveau réseau privé détecté* s'affiche comme suit:

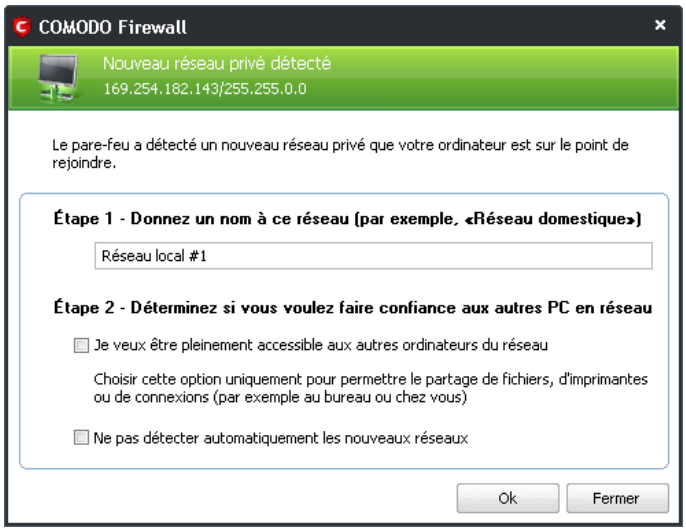

COMODO Firewall
Nouveau réseau privé détecté
169.254.182.143/255.255.0.0
Le pare-feu a détecté un nouveau réseau privé que votre ordinateur est sur le point de rejoindre.
Étape 1 - Donnez un nom à ce réseau (par exemple, «Réseau domestique»)
Réseau local #1
Étape 2 - Déterminez si vous voulez faire confiance aux autres PC en réseau
Je veux être pleinement accessible aux autres ordinateurs du réseau
Choisir cette option uniquement pour permettre le partage de fichiers, d'imprimantes ou de connexions (par exemple au bureau ou chez vous)
Ne pas détecter automatiquement les nouveaux réseaux
Ok
Fermer

Figure 7: La fenêtre Nouveau réseau privé détecté de COMODO Firewall

Astuce: Si vous travaillez dans un environnement LAN, cochez l'option *Je veux être pleinement accessible aux autres ordinateurs du réseau* pour activer les fonctions de partage de fichiers/dossiers/imprimantes et/ou de connexion à Internet.

Dixième étape. Dans le champs *Donnez un nom à ce réseau*, **saisissez** un nouveau nom ou acceptez le nom par défaut tel qu'illustré à la *Figure 7* ci-dessus. Laissez les options de la rubrique *Étape 2 - Déterminez si vous voulez faire confiance aux autres PC en réseau* dessélectionnez, puis **cliquez** sur OK pour finaliser l'installation.

L'icone de bureau **COMODO Firewall** et l'icone de connectivité **COMODO Firewall** apparaissent en même temps que la fenêtre illustrée à la *figure 7*. Avant de vous connecter à Internet, l'icone de connectivité s'affiche dans la barre des tâches, tel qu'illustré ci-dessous:

Figure 8: L'icone de connectivité de COMODO Firewall (ici surligné en noir) dans la barre des tâches

Lorsque une requête est faite pour aller sur Internet ou lancer un programme qui doit accéder à Internet (par exemple, un navigateur Web), une série de flèches orange pointant vers le bas et de flèches verte pointant vers le haut s'afficheront pour indiquer toute requête de connexion entrante ou sortante à Internet, tel qu'illustré ci-dessous:

Figure 9: L'icone de connectivité de COMODO Firewall en action

Après quelques minutes de fonctionnement, le *Centre de messagerie de COMODO* affichera peut-être un message comme celui-ci:

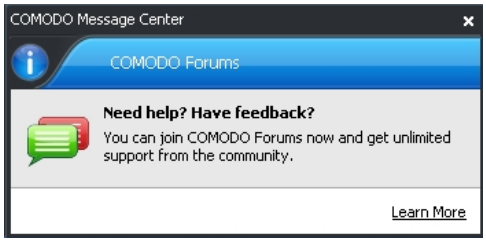

COMODO Message Center
COMODO Forums
Need help? Have feedback?
You can join COMODO Forums now and get unlimited support from the community.
Learn More

Figure 10: La fenêtre du Centre de messagerie de COMODO

Commentaire: **Cliquez** sur le lien *Learn more* pour être automatiquement redirigé vers les forums d'aide de **Comodo**.

Astuce: **Cliquez à droite** sur l'icone de connectivité de **COMODO Firewall** dans la *Barre des tâches* (tel qu'illustré à la *figure 10*) pour afficher le menu contextuel suivant, ainsi que ses sous-menus:

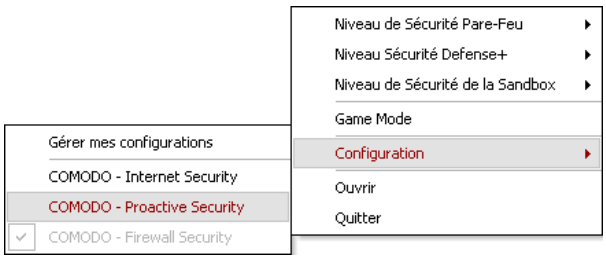


Figure 11: Le menu et les sous-menus contextuels de l'icone de connectivité

Le menu de l'icone de connectivité vous permet de changer les produits de **COMODO Firewall** que vous utilisez. En **sélectionnant** l'item *Configuration*, vous activez le sous-menu *Gérer mes configurations*, où vous pouvez **sélectionner** soit *COMODO - Proactive Security*, soit *COMODO - Internet Security* afin d'activer la fonction 'Sandbox'.

De plus, il est possible d'ajuster le niveau de sécurité de chaque produit à partir du menu contextuel de l'icone de connectivité, tel qu'illustré ci-dessous; ces niveaux de sécurité sont examinés plus attentivement dans les sections **4.1 La fenêtre de réglages du comportement du pare-feu** et **4.2 La fenêtre de réglages de Defense+**

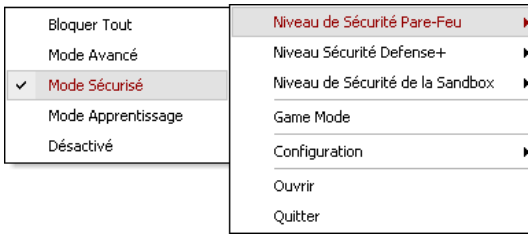


Figure 12: Le sous-menu 'Niveau de sécurité Pare-feu' de l'icone de connectivité

Comment utiliser COMODO Firewall

Sommaire des sections de cette page:

- **3.0 Comment autoriser ou bloquer des accès avec COMODO Firewall**
- **3.1 Comment ouvrir l'interface principale de COMODO Firewall**
- **3.2 Un survol de l'interface principale de COMODO Firewall**

3.0 Comment autoriser ou bloquer des accès avec COMODO Firewall

Un pare-feu est un programme conçu pour protéger votre ordinateur contre des pirates ou des logiciels malveillants. Ces derniers peuvent tenter d'accéder directement à votre ordinateur ou d'envoyer des donnée à partir de votre ordinateur vers une tierce partie. **Comodo Firewall** doit être configuré correctement pour lui permettre d'apprendre et d'enregistrer quelles sont les applications qui sont "sûres" afin de leur autoriser l'accès, et de bloquer les requêtes provenant de logiciels dangereux et/ou constituent des menaces.

Chaque fois que **Comodo Firewall** reçoit une requête de connexion, il affiche une fenêtre *Alerte Pare-feu* vous demandant d'*autoriser* ou de *bloquer* l'accès de votre système depuis ou vers l'Internet. L'exercice qui suit concerne un programme sûr (**Firefox**) et vous aidera à vous familiariser avec les alertes pare-feu et à les utiliser correctement. Même si des exceptions sont parfois faites pour les requêtes provenant de navigateurs et clients de courrier électronique universellement reconnus, chaque fois qu'une requête de connexion est faite, une *Alerte pare-feu* semblable à celle-ci s'affiche:

COMODO Alerte Pare-Feu
firefox.exe is trying to connect to the Internet
Application : firefox.exe
Distant : 127.0.0.1 - TCP
Port : 12080
Considérations de sécurité
firefox.exe is a safe application signed by Mozilla Corporation.
Vous pouvez sans risque accepter cette demande.
Se souvenir de ma réponse
Plus d'options
Que dois-je faire ?
Autoriser
Bloquer

Figure 1: Un exemple d'alerte pare-feu de COMODO

Un pare-feu n'est rien d'autre qu'un ensemble de règles servant à contrôler le trafic entrant et sortant. Chaque fois que vous cliquez sur *Autoriser* ou *Bloquer*, **COMODO Firewall** génère une règle sur mesure pour la requête au réseau de ce processus ou de ce programme. **COMODO Firewall** fait cela pour les processus et programmes nouveaux ou inconnus, ainsi que pour ceux compris dans la liste *Éditeurs de logiciels certifiés* de la fenêtre *Defense+ - Tâches > Stratégie de Sécurité*.

Se souvenir de ma réponse: Cette option est employée pour enregistrer si autorisez ou bloquez un programme en particulier. **COMODO Firewall* autorisera ou bloquera automatiquement les requêtes provenant de ce programme la prochaine fois qu'il tentera de se connecter, selon le choix que vous aurez fait préalablement.

Important: Nous recommandons fortement de désactiver la fonction *Se souvenir de ma réponse* lorsque vous commencez à utiliser **COMODO Firewall**. Décidez si vous autorisez ou bloquez différentes requêtes et observez quels effets vos décisions ont sur le fonctionnement de votre système. Activez la fonction *Se souvenir de ma réponse* si et *seulement si* vous êtes complètement sûr de votre décision.

Astuce: Limiter strictement l'accès à votre système est la meilleure façon d'en assurer la sécurité. N'hésitez pas à bloquer toutes les requêtes suspectes ou non identifiées. Si un blocage fait en sorte qu'un programme ne fonctionne plus normalement, vous pourrez autoriser la requête la prochaine fois que vous recevez une alerte du pare-feu.

Première étape. **Cliquez** sur Application : firefox.exe pour afficher la fenêtre *Propriétés* et obtenir des renseignements sur le processus ou le programme qui lance une requête, dans ce cas-ci, **Firefox**:

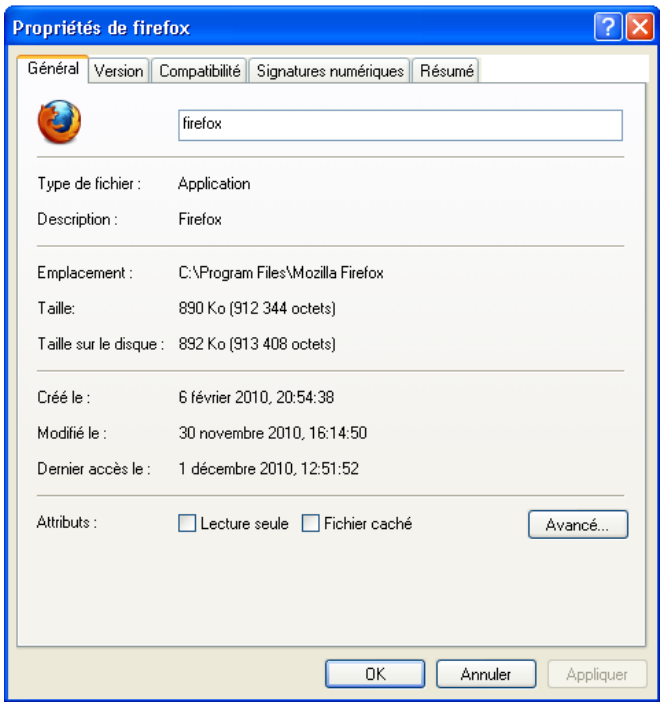


Figure 2: La fenêtre Propriétés de Firefox.exe

Deuxième étape: **Cliquez** sur OK pour fermer la fenêtre *Propriétés* du programme.

Troisième étape: Selon les renseignements affichés dans la fenêtre *Propriétés*: si vous avez déterminé qu'une requête n'est pas sûre, ou si vous êtes incertain, **cliquez** sur Bloquer pour donner à **COMODO Firewall** la consigne de bloquer l'accès à votre système. OU: Si vous avez déterminé qu'un programme légitime lance une requête non malveillante, **cliquez** sur Autoriser pour autoriser l'accès à votre système.

Quatrième étape. **Cliquez** sur Autoriser pour permettre à **Firefox** d'accéder à votre système par l'intermédiaire de **COMODO Firewall**.

Cinquième étape. Puisque **Firefox** est un programme considéré sûr, **cochez** l'option Se souvenir de ma réponse pour que **COMODO Firewall** autorise automatiquement l'accès à **Firefox** la prochaine fois et subséquemment.

Commentaire: Le bouton *Autoriser* vous permet d'autoriser manuellement, au cas par cas, l'accès à un processus ou un programme.

Astuce: **Cliquez** sur Que dois-je faire ? pour accéder aux fiches d'aide en ligne de **COMODO Firewall**.

Votre capacité à prendre les bonnes décisions s'améliorera au fur et à mesure que vous prendrez de l'expérience avec **COMODO Firewall**.

3.1 Comment ouvrir l'interface principale de COMODO Firewall

COMODO Firewall démarrera automatiquement lorsque vous aurez installé le programme et redémarré votre système. Le programme comporte un panneau de configuration complet, avec de nombreuses fonctions et options flexibles. Les utilisateurs **débutants** apprendront facilement à gérer les alertes de sécurité **COMODO Firewall**, alors que les utilisateurs *expérimentés* et *avancés* pourront se familiariser avec des aspects plus complexes de la gestion et de la configuration du pare-feu.

Commentaire: Tous les exemples illustrés ici sont basés sur le mode *Défense optimale*. Cela signifie que le système de prévention des intrusions est activé automatiquement. Si vous avez installé **COMODO Firewall** avec l'option *Pare-feu seulement*, *Defense+"* ne sera pas activé.

Pour ouvrir l'interface principale de **COMODO Firewall** suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Démarrer> Programmes > Comodo > Firewall > Comodo Firewall**.

Commentaire: Vous pouvez également afficher l'interface principale du programme en **double-cliquant** sur l'icone de bureau, ou en **double-cliquant** sur l'icone **COMODO Firewall** qui se trouve dans la *Barre des tâches*. De plus, vous pouvez **cliquer à droite** sur l'icone **COMODO Firewall** pour afficher le menu contextuel, puis **sélectionner** *ouvrir*, comme suit:

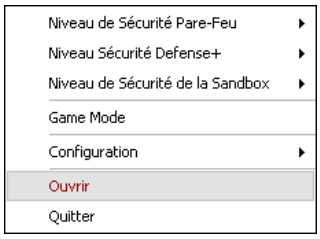


Figure 3: Le menu contextuel à partir de l'icone de connectivité COMODO Firewall

Figure 4: L'interface principale de Comodo Firewall, en mode Sommaire par défaut

3.2 Un survol de l'interface principale de COMODO Firewall

La fenêtre *Pare-feu* affiche un sommaire clair et concis des requêtes entrantes et sortantes des processus et programmes qui tentent de se connecter par l'entremise de **COMODO Firewall**. Il y a habituellement davantage de requêtes sortantes que de requêtes entrantes. Le mode de fonctionnement par défaut est le *Mode sécurisé*. Les différents modes seront abordés plus loin dans cette section. Le *Trafic* affiche les différents processus et programmes en cours et le nombre de requêtes effectuées, sous forme de pourcentage.

Cliquez sur

pour afficher les sommaires détaillés des requêtes sortantes *en tout temps*, comme suit:

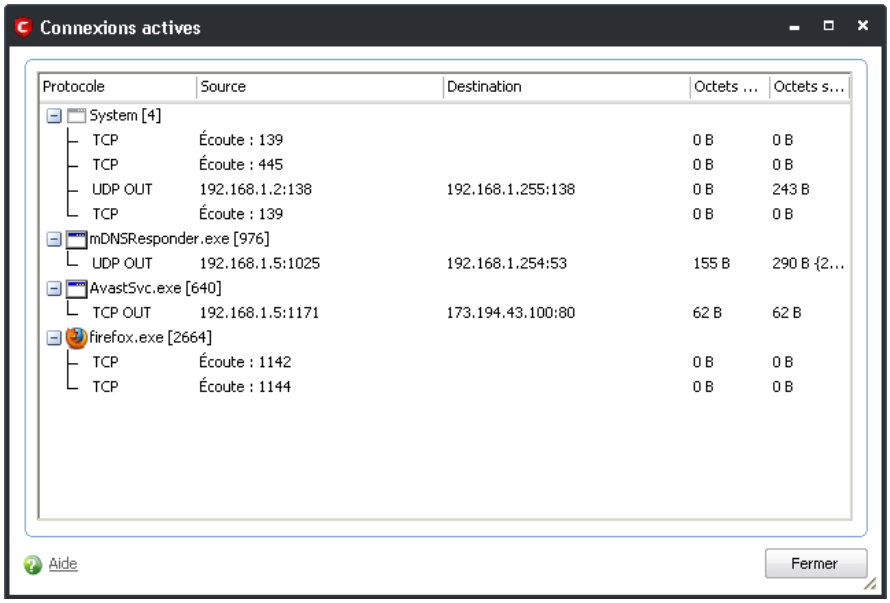

Connexions actives
Protocole
Source
Destination
Octets ...
Octets s...
System [4]
TCP Écoute : 139 0 B 0 B
TCP Écoute : 445 0 B 0 B
UDP OUT 192.168.1.2:138 192.168.1.255:138 0 B 243 B
TCP Écoute : 139 0 B 0 B
mDNSResponder.exe [976]
UDP OUT 192.168.1.5:1025 192.168.1.254:53 155 B 290 B (2...
AvastSvc.exe [640]
TCP OUT 192.168.1.5:1171 173.194.43.100:80 62 B 62 B
firefox.exe [2664]
TCP Écoute : 1142 0 B 0 B
TCP Écoute : 1144 0 B 0 B
Aide
Fermer

Figure 5: Un exemple de fenêtre de Connexions actives affichant les détails du trafic Internet

Cliquez sur 1 connexion(s) entrante(s) pour afficher la fenêtre des *Connexions actives* des requêtes entrantes, *en tout temps*.

Astuce: **Cliquez** sur Stopper Tout Trafic pour arrêter toutes les requêtes entrantes et sortantes, si votre service Internet ralentit ou plante soudainement, et/ou si vous avez des raisons de croire qu'un processus ou un programme malveillant est en cours de téléchargement ou d'opération. Ce faisant, vous mettez automatiquement le *pare-feu* en mode de fonctionnement Bloquer Tout. Révisez le sommaire détaillé dans la fenêtre *Connexions actives* pour trouver les possibles sources du problème.

Après vous être assuré d'avoir résolu les problèmes, **cliquez** sur Ré-autoriser Tout Trafic pour indiquer à **COMODO Firewall** de recommencer à traiter les requêtes entrantes et sortantes et retourner au Mode sécurisé comme d'habitude.

3.2.1 Les icones d'état de COMODO Firewall

COMODO Firewall et **Defense+** fonctionnent main dans la main; si les deux programmes sont en cours d'opération, l'icone qui se trouve à la gauche de l'interface principale s'affiche comme suit:

Figure 6: L'icone d'état vert de COMODO Firewall

Si l'un ou l'autre des programmes est désactivé, l'icone d'état indique que le pare-feu ou une des composants de la protection proactive est désactivé:

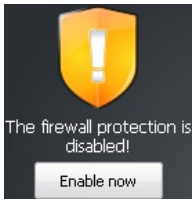


Figure 7: L'icone d'état jaune indiquant que le pare-feu est désactivé

Si les deux programmes sont désactivés, l'icone d'état s'affiche comme suit:

Figure 8: L'icone d'état jaune de COMODO Firewall indiquant que plusieurs protections sont désactivées

Dans un cas comme dans l'autre, **cliquez** sur pour activer la protection correspondante.

Configuration et paramètres avancés

Sommaire des sections de cette page:

- **4.0 Comment accéder aux fenêtres Pare-feu et Defense+**
- **4.1 La fenêtre Paramètres du comportement du Pare-feu**
- **4.2 La fenêtre Paramètres Defense+**

4.0 Comment accéder aux fenêtres Pare-feu et Defense+

L'interface principale de **COMODO Firewall** est séparée en deux panneaux, le panneau *Pare-feu* et le panneau *Defense+*.

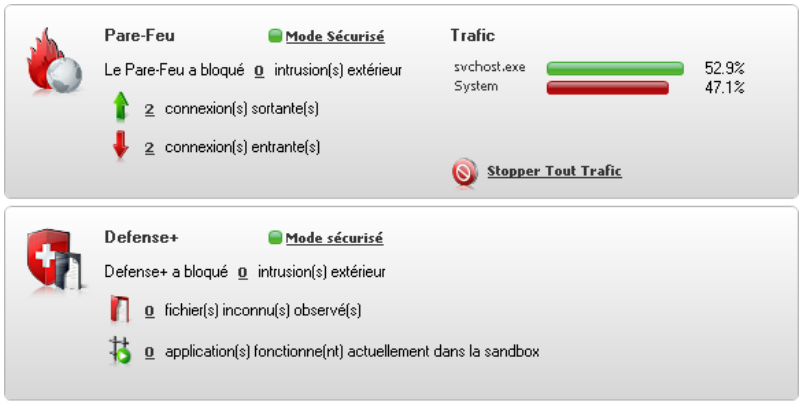


Figure 1: L'interface principale de COMODO Firewall affichant les panneaux Pare-feu et Defense+

On accède aux fenêtres *Paramètres du comportement du Pare-feu* et *Paramètres Defense+* en **cliquant** sur Mode sécurisé

dans l'un ou l'autre des panneaux pour afficher la fenêtre correspondante et les onglets associés.

On peut également accéder à l'une ou l'autre de ces fenêtres en suivant les étapes énumérées ci-dessous:

Première étape. **Ouvrez** l'interface principale de **COMODO Firewall**.

Deuxième étape. **Cliquez** sur

pour afficher la fenêtre *Tâches du Pare-feu* ou *Tâches Defense+*, respectivement.

Troisième étape. **Cliquez** sur

Paramètres du comportement du Pare-feu
Accéder et configurer les différentes options de pare-feu (niveau de sécurité, niveau de fréquence d'alerte, ...).
OU
Paramètres Defense+
Vous pouvez utiliser cette section pour modifier différents réglages qui permet à Defense+ operate according to specific defense requirements of the computer.

Pour afficher le contenu de l'onglet *Paramètres du comportement du pare-feu* OU celui de l'onglet *Paramètres Defense+*, respectivement.

Astuce: Les *Niveau de Sécurité Pare-feu*, *Niveau de Sécurité Defense+* et *Niveau de Sécurité de la Sandbox*, qui sont abordés dans la prochaine section, peuvent être réglés facilement et efficacement en passant par l'icone de connectivité de **COMODO Firewall** qui se trouve dans la *Barre des tâches* Windows. **Cliquez à droite** sur l'icone de connectivité pour afficher le menu contextuel et les sous-menus, tel qu'illustré ci-dessous:

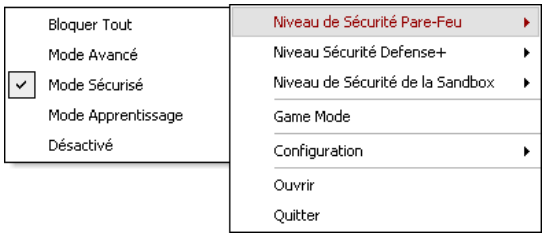


Figure 2: Le menu contextuel de l'icone de connectivité affichant le niveau de sécurité du Pare-feu

4.1 La fenêtre des paramètres du comportement du Pare-feu

La fenêtre **Paramètres du comportement du Pare-feu vous permet de personnaliser le pare-feu avec une panoplie d'options et de fonctionnalités, dont le niveau de sécurité du pare-feu, la fréquence et le type d'alertes à recevoir, ainsi que l'analyse et la surveillance des paquets.

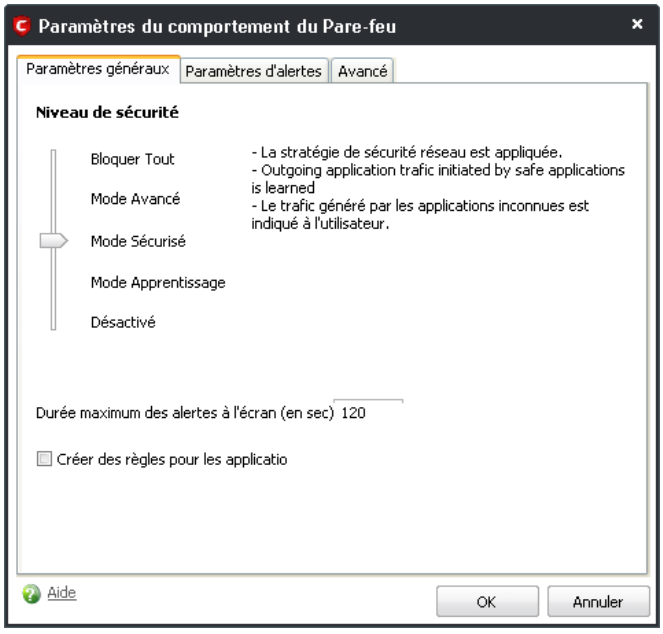


Figure 3: La fenêtre Paramètres du comportement du pare-feu - Paramètres généraux

L'onglet *Paramètres généraux* vous permet de spécifier le niveau de sécurité que vous jugez approprié pour **COMODO Firewall**. Le glisseur vous permet de choisir parmi les niveaux de sécurité suivants: toutes **Bloquez tout**: Ce mode bloque tout le trafic Internet et outrepasse tous les réglages et toutes les règles que vous avez déterminées. Ce mode ne génère aucune règle de trafic pour les applications et n'enregistre pas leur comportement.

Mode avancé: Ce mode applique *uniquement* les stratégies de sécurité et de réseautage déterminées par l'utilisateur dans les fenêtres *Tâches Pare-feu > Stratégie de Sécurité Réseau* et *Tâches Dedense+ > Stratégie de Sécurité*.

Mode sécurisé: Ce mode est le réglage par défaut de **COMODO Firewall**, y compris les installations *Défense proactive*

optimale et *Défense proactive maximale*.

Astuce: **COMODO Firewall** maintient une liste interne des applications et fichiers régulièrement utilisés qui ont été définis comme sûrs, et n'émet pas d'alertes pour ceux-ci.

Avertissement: Les modes *Apprentissage* et *Désactivé* ne sont pas recommandés car ils peuvent nuire à l'efficacité de **COMODO Firewall** et exposer votre ordinateur à des risques d'infection.

4.2 La fenêtre Paramètres Defense+

Commentaire: Les fonctionnalités et options décrites dans cette section exigent une compréhension approfondie des pare-feu et des questions de sécurité, et est par conséquent principalement conçu pour les utilisateurs de niveau *avancé*.

Important: si vous avez coché l'une ou l'autre des options **Pare-feu avec défense proactive optimale*** et ***Pare-feu avec défense proactive maximale*** **lors du processus d'installation de **COMODO Firewall**, le système de prévention des intrusions *Defense+* a été automatiquement activé. Cela dit, si vous avez coché l'option *Pare-feu seulement*, le système *Defense+* peut tout de même être activé manuellement. L'option *Defense+* doit être activée pour que plusieurs des fonctionnalités décrites ci-dessous soient en mesure de fonctionner.

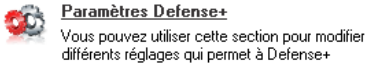
La fonction *Defense+* de **COMODO Firewall** est un système de prévention des intrusions. Tout ordinateur connecté à un réseau est techniquement un ordinateur hôte. Le système *Defense+* surveille continuellement les activités de tous les fichiers exécutables qui se trouvent actuellement sur votre ordinateur. Un fichier exécutable est une application ou un programme, ou une partie d'un programme, est est habituellement (mais pas nécessairement) identifiable par l'un ou l'autre des extensions de fichiers suivants: *.bat*, *.exe*, *.dll*, *.sys*, ou d'autres.

Defense+ émet des alertes chaque fois qu'un fichier exécutable inconnu tente de s'exécuter, et vous demande d'autoriser ou de bloquer son exécution. Ce système peut s'avérer important dans les situations où des logiciels malveillants essaieraient d'installer des applications ou des programmes pour endommager ou voler vos données personnelles, reformater votre disque dur ou détourner votre système pour propager des programmes malveillants ou du pourriel sans votre consentement ou votre connaissance.

4.2.1 La fenêtre Paramètres Defense+ - Onglet Paramètres généraux

Pour activer manuellement le système *Defense+* et afficher la fenêtre *Paramètres Defense+*, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur l'onglet *Defense+* dans l'interface principale de **COMODO Firewall**, puis **cliquez** sur



pour afficher la fenêtre suivante:

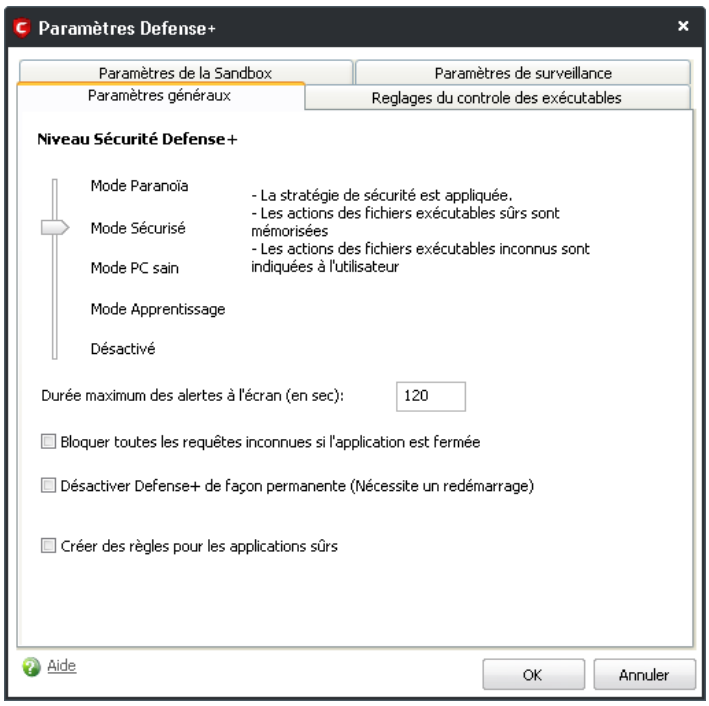
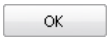

Paramètres Defense+
Paramètres de la Sandbox
Paramètres de surveillance
Paramètres généraux
Reglages du controle des exécutables
Niveau Sécurité Defense+
Mode Paranoïa
Mode Sécurisé
Mode PC sain
Mode Apprentissage
Désactivé
- La stratégie de sécurité est appliquée.
- Les actions des fichiers exécutables sûrs sont mémorisées
- Les actions des fichiers exécutables inconnus sont indiquées à l'utilisateur
Durée maximum des alertes à l'écran (en sec):
120
Bloquer toutes les requêtes inconnues si l'application est fermée
Désactiver Defense+ de façon permanente (Nécessite un redémarrage)
Créer des règles pour les applications sûrs
Aide
OK
Annuler

Figure 6: La fenêtre Defense+ affichant l'onglet Paramètres général par défaut

Deuxième étape. **Faites passer** le glisseur au *Mode sécurisé*, puis **cliquez** sur 

pour activer le système *Defense+* tel qu'illustré à la *Figure 6*.

Le *Niveau de Sécurité Defense+* ressemble au *Niveau de sécurité du comportement du Pare-feu*, offre des options similaires, et vous permet d'utiliser le glisseur pour choisir le niveau de protection optimal contre les intrusions.

Mode Paranoïa: Ce mode offre le niveau de sécurité le plus élevé; il comprend une surveillance automatique de tous les fichiers exécutables, à part ceux que vous avez définis comme sûrs, y compris ceux inclus dans la liste des *Éditeurs de logiciels certifiés*. Ce mode comporte la plus haute fréquence d'alertes de sécurité, et l'activité du système est filtrée à travers les paramètres de votre configuration.

Mode sécurisé: Ce mode 'apprend' automatiquement les comportements des différentes applications exécutables, tout en surveillant les activités critiques du système. Toutes les applications non certifiées génèrent une *Alerte de sécurité* chaque fois

qu'elles sont mises en exécution. Ce mode est le plus recommandé pour la majorité des utilisateurs.

- L'option *Bloquer toutes les requêtes inconnues si l'application est fermée* bloque automatiquement toutes les requêtes émises par des applications et des programmes inconnus, ou que vous n'avez pas spécifié dans votre *Stratégie de sécurité*.
- L'option *Désactiver Defense+ de façon permanent (nécessite un redémarrage)* vous permet de désactiver manuellement le système de prévention des intrusions * Defense+*. Cette option n'est généralement pas recommandée.

4.2.2 Les paramètres Defense+ - Onglet Réglages du contrôle des exécutables

L'onglet *Réglages du contrôle des exécutables* limite l'auto-exécution des fichiers suspects ou inconnus (ainsi que leur accès aux ressources de votre ordinateur), et soumet ceux-ci à une analyse.

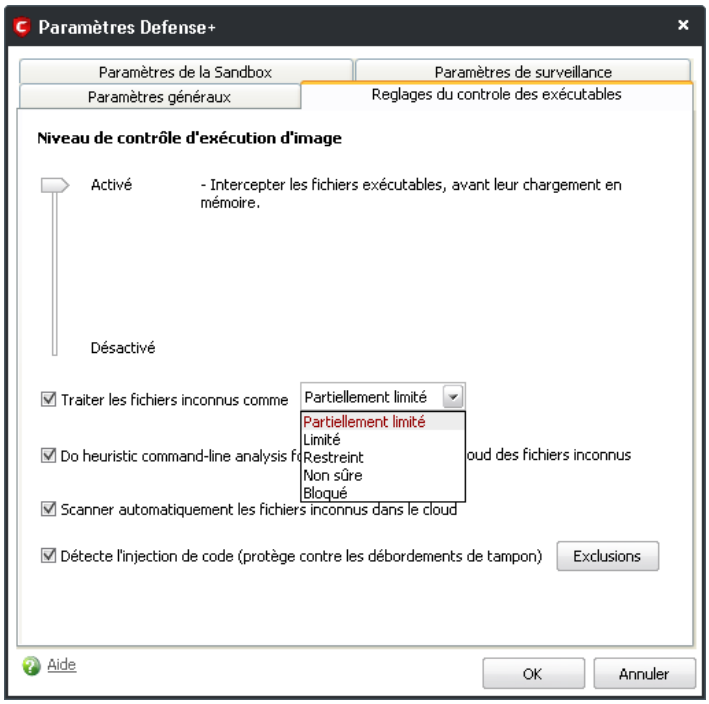


Figure 7: L'onglet Réglages du contrôle des exécutables

Astuce: Les utilisateurs de niveau **avancé** peuvent créer des exclusions aux tâches susmentionnées en cliquant sur Exclusions pour afficher le panneau *Exclusions* et sélectionner différents processus et programmes à exclure.

Commentaire: Les utilisateurs de niveau **expérimenté** et **avancé** sont fortement encouragés à **cliquer** sur Aide pour accéder aux fiches d'aide en ligne de **COMODO** qui concernent les onglets *Réglages du contrôle des exécutables*, les *Paramètres de la Sandbox* et les *Paramètres de surveillance*. Vous pouvez également vous référer à **http://help.comodo.com/topic-72-1-155-1074-Introduction-to-Comodo-Internet-Security.html** pour choisir une fiche à partir d'une liste de rubriques d'aides en ligne.

Faq et questions récapitulatives

5.0 Faq et questions récapitulatives

Muhindo et Salima sont agréablement surpris de constater à quel point **COMODO Firewall** est facile à utiliser et fonctionne silencieusement en arrière-plan. Il leur reste cependant quelques questions.

Q: *Si je n'ai pas de pare-feu, peux-tu me parler davantage des menaces qui guettent mon ordinateur? Quels sont les différents types de programmes qui peuvent accéder à mon ordinateur, et que font-ils?*

A: *Il existe des milliers de programmes qui peuvent accéder à ton ordinateur depuis Internet s'il n'y a pas de pare-feu installé. Il existe même des "araignées" du Web (ou robots) qui parcourent toutes les adresses possibles à la recherche d'ordinateurs qui ne sont pas munis d'un pare-feu fonctionnel. Lorsqu'elles trouvent ces adresses, les araignées les rapportent aux pirates. De plus, il existe des programmes conçus pour 'détourner' ton ordinateur et l'utiliser pour mener des transactions illégales ou disséminer du pourriel sans ton consentement ou ta connaissance: tu pourrais potentiellement être accusé pour des activités illégales dont tu es complètement innocent!*

Q: *Si **COMODO Firewall** garde tous ces programmes à distance, pourquoi ai-je aussi besoin d'un programme antivirus et d'un programme anti-logiciel espion?*

A: *Un pare-feu se concentre sur la restriction de l'accès depuis et vers Internet. Il empêche un programme ou un pirate d'accéder à ton ordinateur, mais ne peut pas te protéger des logiciels malveillants qui sont téléchargés, par exemple, par messagerie électronique, depuis des sites Internet ou depuis des disques externes. **COMODO Firewall** comprend en outre **Defense+**, un système de prévention des intrusions qui surveille en permanence les types de fichiers exécutables autorisés à fonctionner sur notre système. Les programmes antivirus et anti-logiciel espion servent à empêcher la contamination là où le pare-feu est impuissant. De plus, ces outils peuvent également retirer des logiciels malveillants déjà installés sur ton ordinateur.*

Q: *Devrais-je être vigilant à l'égard de logiciels malveillants qui ont l'apparence de programmes Windows (ou d'autres*

programmes inoffensifs)?

A: *Malheureusement, de nombreux programmes sont conçus ainsi. Tu dois être très vigilant quant à l'origine d'un programme lorsque tu le télécharges ou l'installes. Tu ne devrais installer aucun logiciel qui n'est pas absolument utile et nécessaire à ton travail, surtout sur des ordinateurs qui contiennent beaucoup de données importantes ou délicates. C'est à cet égard que le système de prévention des intrusions* ***COMODO Defense+*** *peut s'avérer fort utile; en comparant chaque nouvel exécutable des applications récemment installées avec une liste d'éditeurs de logiciels certifiés et en soumettant à l'analyse tout logiciel potentiellement malveillant, cet outil améliore considérablement ta sécurité sur Internet.*

Q: *Dans quelle mesure* ***COMODO Firewall*** *offre-t-il une protection efficace contre les pirates?*

A: ***COMODO Firewall*** *offre un contrôle complet et raffiné de l'accès à la plateforme *Windows*.* Cela dit, un pare-feu n'est efficace que dans la mesure où sa configuration est appropriée. En dépit des inconvénients mineurs que présentent un pare-feu, il est fortement recommandé de persister dans son utilisation. Continue à t'informer sur **COMODO Firewall**; plus tu sera familier avec le programme, plus tu comprendras à quel point la protection qu'il t'offre est avantageuse.*

5.1 Questions récapitulatives

- Peut-on employer plus d'un pare-feu à la fois?
- Comment peut-on vérifier si un programme avec lequel on n'est pas familier est suffisamment sûr pour le laisser s'exécuter sur notre ordinateur?
- Comment le pare-feu fonctionne-t-il?
- Quelle est la différence entre un pare-feu et un système de prévention des intrusions?
- Pourquoi dois-je installer un pare-feu?

KeePass - stockage de mots de passe

Short Description:

KeePass est un outil de gestion de mots de passe sécurisé et facile à utiliser.

Online Installation Instructions:

Pour télécharger KeePass

- *Lisez la courte introduction aux* ***Guides pratiques*** *[1]*
- ***Cliquez*** *sur l'icone* ***KeePass****ci-dessous pour ouvrir la page de téléchargement www.keepass.info/download.html*
- *Dans la section "****Classic Edition****", cliquez sur "****KeePass 1.xx (Installer EXE for Windows)****".*
- *Sauvegardez le fichier d'installation KeePass-1.xx-Setup.exe à un emplacement de votre choix, puis cliquez dessus pour lancer l'installation.*
- *Vous pouvez supprimer l'exécutable après l'installation.*

Keepass:

[49]

Pour utiliser KeePass en français

- **Installez KeePass** en suivant les consignes indiquées à la section **2.0 Comment installer Keepass** [50]
- Rendez-vous à la **page web des traductions de KeePass** [51]
- Localisez le fichier .zip de traduction française **French-1.xx.zip** et sauvegardez-le sur votre ordinateur à un emplacement de votre choix.
- Décompactez le fichier .zip, et copiez le fichier *French.lng* dans le répertoire où **KeePass** est installé (habituellement C:/Program Files/KeePass).
- **Démarrez KeePass**, allez au menu *View* > *Change Language...* et **sélectionnez** *French*.
- Redémarrez KeePass.

Site Internet

www.keepass.info [52]

Configuration requise

- Compatible avec toutes les versions de Windows

Version utilisée pour rédiger ce guide

- 1.18

Licence

- Free/libre Open Source Software (FLOSS)

Lecture préalable

- Livret pratique Security in-a-box, chapitre **3. Créer et sauvegarder des mots de passe sûrs** [53].

Niveau: 1 : Débutant, **2 : Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

Temps d'apprentissage: 15 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de sauvegarder tous vos mots de passe dans une seule base données (une base de mots de passe) pratique et sécurisée.
- La capacité de créer et de stocker plusieurs mots de passe forts (complexes) sans pour autant devoir les mémoriser.

Autres programmes compatibles avec GNU Linux, Mac OS et Microsoft Windows:

KeePass est également compatible avec **GNU Linux** et **Mac OS** (dans sa version **KeePassX** [54] version). Il existe aussi des versions de **KeePass** pour d'autres plateformes, comme **iPhone**, **BlackBerry**, **Android**, **PocketPC**, etc. Si vous préférez essayer d'autres programmes similaires, nous recommandons:

- **Password Safe** [55], compatible avec **Microsoft Windows** et **GNU Linux**
- **1Password** [56] compatible avec **Mac OS**, **Microsoft Windows**, **iPhone** et**iPad**

1.1 À propos de cet outil

KeePass est un outil puissant et facile à utiliser qui vous permettra de stocker et de gérer vos mots de passe dans une base de données, ou base de mots de passe, hautement sécurisée. Il vous sera possible de charger la base de mots de passe et le programme **KeePass** sur une clé USB que vous pourrez transporter sur vous. La base de mots de passe est protégée par un mot de passe principal que vous créez vous-même. Ce mot de passe unique sert à chiffrer l'ensemble du contenu de la base de mots de passe. Vous pouvez stocker vos mots de passe existants avec **KeePass** ou vous servir du logiciel pour en générer de nouveaux. KeePass ne requiert aucune configuration préalable et ne comporte pas d'instructions d'installation particulières. Le logiciel peut être utilisé aussitôt que VOUS êtes prêts à le faire!

Comment utiliser KeePass

Sommaire des sections de cette page:

- **2.0 Comment installer KeePass**
- **2.1 Comment créer une nouvelles base de mots de passe**
- **2.2 Comment ajouter une entrée**
- **2.3 Comment éditer une entrée**
- **2.4 Comment générer des mots de passe aléatoirement**
- **2.5 Comment fermer, réduire ou restaurer KeePass**
- **2.6 Comment créer une copie de sauvegarde de la base de mots de passe**
- **2.7 Comment réinitialiser votre mot de passe principal**

2.0 Comment installer KeePass

Première étape. **Double-cliquez** sur KeePass-1.18-Setup ; si la boîte de dialogue *Fichier ouvert - avertissement de sécurité* s'affiche, **cliquez** sur [Exécuter] pour afficher la fenêtre suivante:

Figure 1: La fenêtre Langue de l'assistant d'installation

Deuxième étape. **Cliquez** sur [OK] pour afficher la fenêtre *Installation - KeePass Password Safe – Bienvenue dans l'assistant d'installation de KeePass Password Safe*.

Troisième étape. **Cliquez** sur [Suivant >] pour afficher la fenêtre *Accord de licence*. Veuillez lire attentivement l'*Accord de licence* avant de poursuivre le processus d'installation.

Quatrième étape. **Cochez** l'option *Je comprends et j'accepte les termes du contrat de licence* pour activer le bouton *Suivant*, puis **cliquez** sur [Next >] pour afficher la fenêtre *Dossier de destination*.

Cinquième étape. **Cliquez** sur [Suivant >] pour accepter l'emplacement par défaut et afficher la fenêtre *Sélection du dossier du menu Démarrer*, puis **cliquez** sur [Suivant >] pour accepter le dossier par défaut.

Sixième étape. **Cliquez** sur [Suivant >] pour afficher la fenêtre suivante:

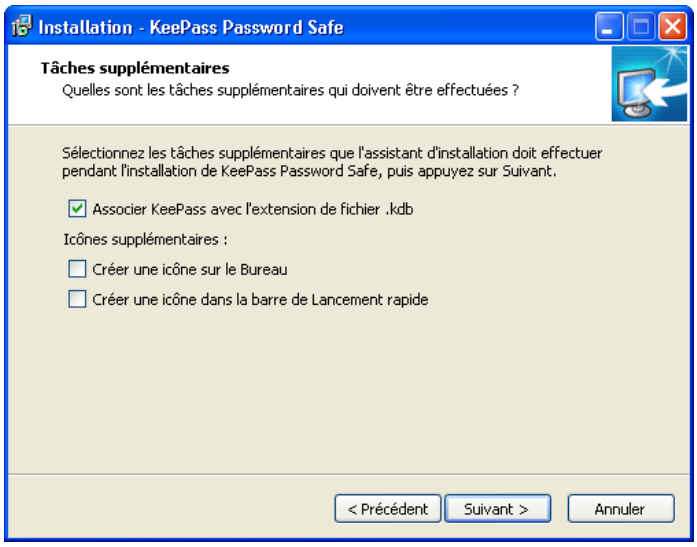

Installation - KeePass Password Safe
Tâches supplémentaires
Quelles sont les tâches supplémentaires qui doivent être effectuées ?
Sélectionnez les tâches supplémentaires que l'assistant d'installation doit effectuer pendant l'installation de KeePass Password Safe, puis appuyez sur Suivant.
Associer KeePass avec l'extension de fichier .kdb
Icônes supplémentaires :
Créer une icône sur le Bureau
Créer une icône dans la barre de Lancement rapide
< Précédent
Suivant >
Annuler

Figure 2: La fenêtre Tâches supplémentaires

Septième étape. **Cochez** l'option Associer KeePass avec l'extension de fichier .kdb tel qu'illustré à la *figure 2*.

Commentaire: Si vous avez laissé l'option *Ne pas créer de dossier dans le menu Démarrer* désactivée à l'étape précédente, l'assistant d'installation de *KeePass Password Safe* crée automatiquement un icone de lancement rapide **KeePass** dans le menu *Démarrer*.

Huitième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Prêt à installer*, puis **cliquez** sur Installer pour afficher la fenêtre **Installation en cours** et sa barre de progression.

Quelques secondes plus tard, la fenêtre *Fin de l'installation de KeePass Password Safe* s'affiche.

Neuvième étape. **Cochez** l'option *Exécuter KeePass*, puis **cliquez** sur Terminer pour ouvrir to **KeePass** immédiatement, ainsi que la page web *Plugins and Extensions* de **KeePass** si vous êtes connecté à Internet.

2.1 Comment créer une nouvelles base de mots de passe

Dans les prochaines sections de ce guide, vous apprendrez à créer un mot de passe principal (clé maître), à sauvegarder la base de mots de passe nouvellement crée, à générer des mots de passe aléatoires pour un programme en particulier, à créer des copies de sauvegarde de votre base de mots de passe et à extraire les mots de passe de **KeePass** lorsque cela s'avère nécessaire.

Pour ouvrir **KeePass**, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez: Démarrer > Programmes > KeePass Password Safe > KeePass** ou **cliquez** sur l'icone de bureau pour afficher la fenêtre principale de **KeePass** illustrée ci-dessous :

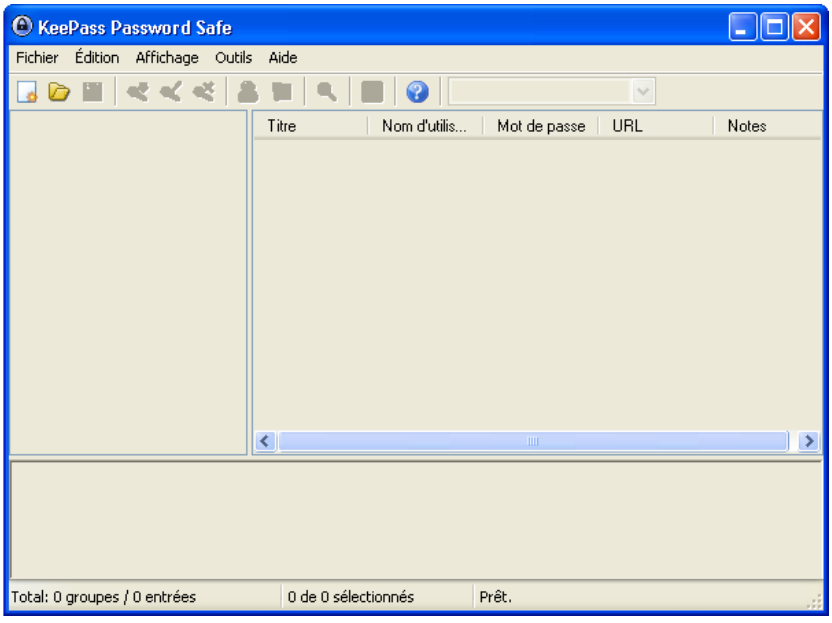


Figure 3: La console de KeePass Password Safe

2.1.1 Comment créer une nouvelles base de mots de passe

La création d'une nouvelle base de mots de passe comporte deux étapes: Vous devez inventer un mot de passe principal, fort (complexe) et unique, qui vous servira à verrouiller et déverrouiller votre banque de mots de passe. Vous devez ensuite

sauvegarder votre banque de mots de passe.

Pour créer une nouvelle base de mots de passe, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez: Fichier> Nouvelle**, comme suit:

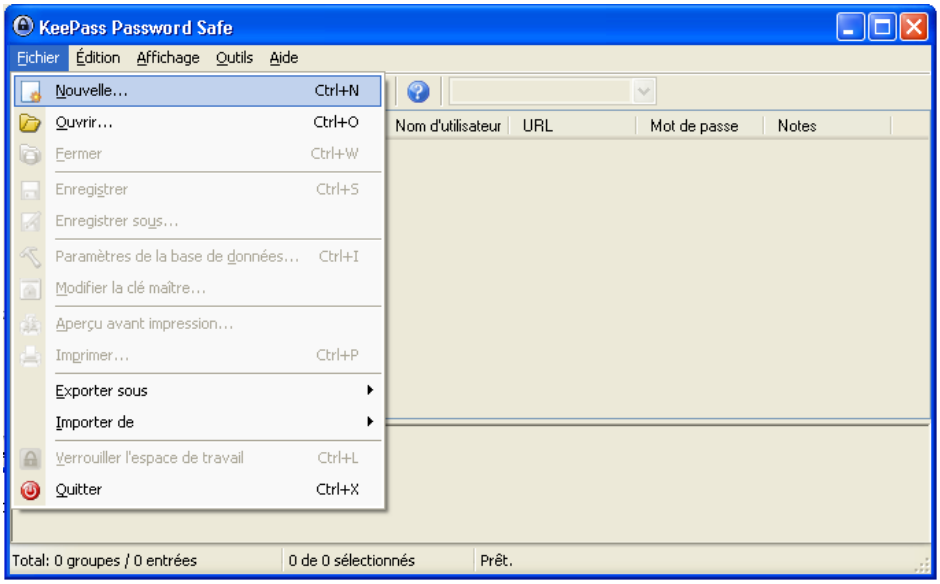


Figure 4: La fenêtre principale de KeePass, avec Fichier > Nouvelle sélectionné

Cela activera la fenêtre *Créer une Nouvelle base de Mots de Passe*, illustrée ci-dessous:

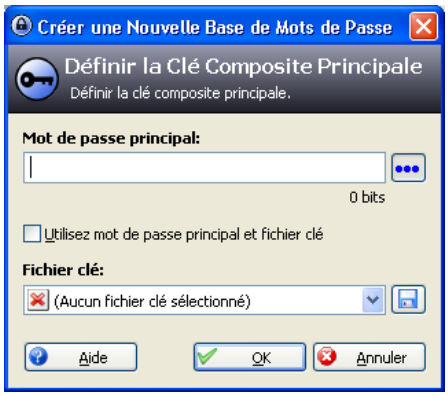


Figure 5: La fenêtre Créer une Nouvelle base de Mots de Passe

Deuxième étape. **Saisissez** le mot de passe maître que vous avez inventé dans la zone *Mot de passe principal*.

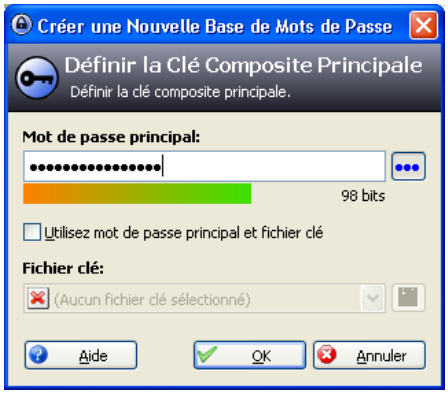
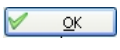


Figure 6: La fenêtre Définir la Clé composite Principale, avec la zone Mot de passe principal remplie

Vous verrez alors apparaître une barre de progression orange/vert sous la saisie du mot de passe. La barre passe du orange au vert au fur et à mesure que vous saisissez votre mot de passe, selon la complexité et la force du mot de passe choisi, et selon le nombre de caractères utilisés.

Astuce: Lorsque vous saisissez votre mot de passe, vous devriez essayer de faire en sorte qu'au moins la moitié de la barre soit colorée en vert.

Troisième étape. **Cliquez** sur  pour activer la fenêtre Confirmer le Mot de passe principal et confirmer votre mot de passe, comme suit:

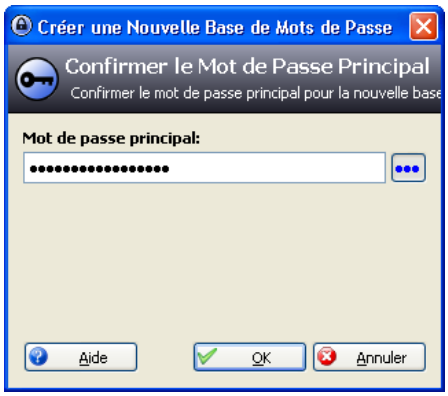

Créer une Nouvelle Base de Mots de Passe
Confirmer le Mot de Passe Principal
Confirmer le mot de passe principal pour la nouvelle base
Mot de passe principal:
Aide
OK
Annuler

Figure 7: La fenêtre Confirmer le Mot de passe principal

Quatrième étape. **Saisissez** le même mot de passe qu'avant, puis **cliquez** sur

Cinquième étape. **Cliquez** sur pour voir si vous avez saisi votre mot de passe correctement.

Attention: Ceci n'est pas recommandé si vous craignez que quelqu'un vous espionne.

Lorsque vous aurez saisi deux fois votre mot de passe maître avec succès, la console principale de **KeePass** sera activée, tel qu'illustré ci-dessous :

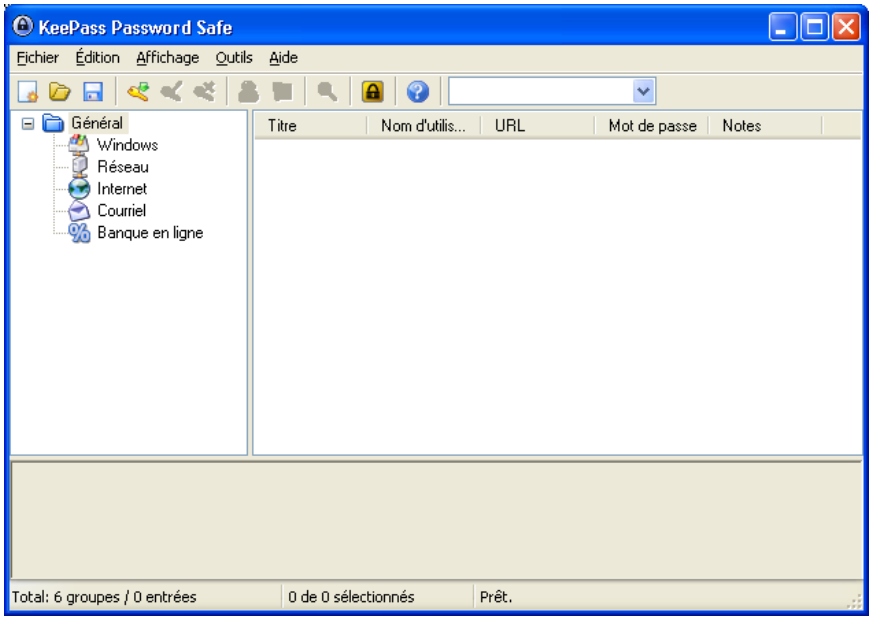


Figure 8: La fenêtre principale de KeePass Password Safe, en mode actif

Lorsque vous aurez créé la base de mots de passe, il vous faudra encore la sauvegarder. Pour sauvegarder la base de mots de passe, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez: Fichier > Enregistrer sous**:

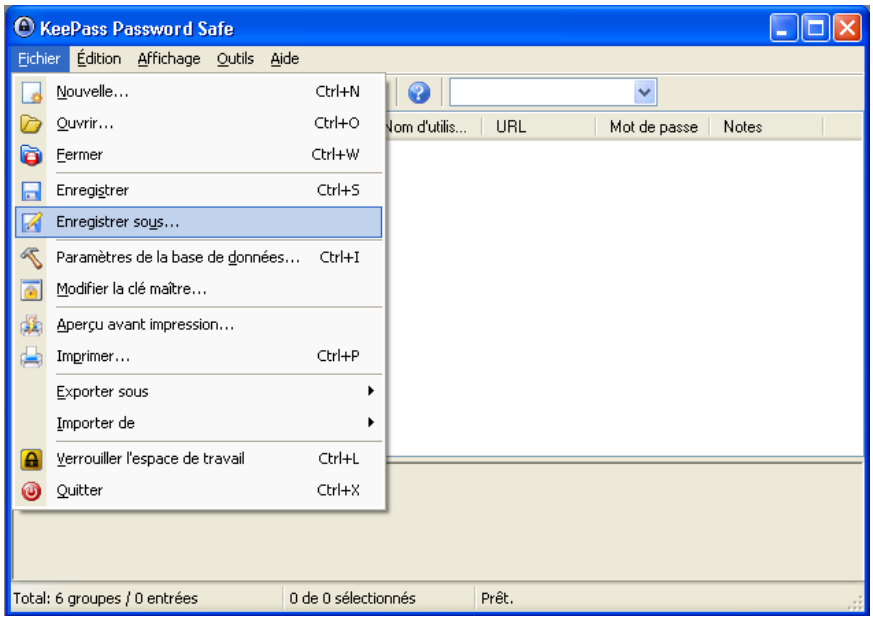


Figure 9: La fenêtre principale de KeePass, avec Fichier > Enregistrez sous sélectionné

Cela activera la fenêtre Enregistrez sous, illustrée ci-dessous:

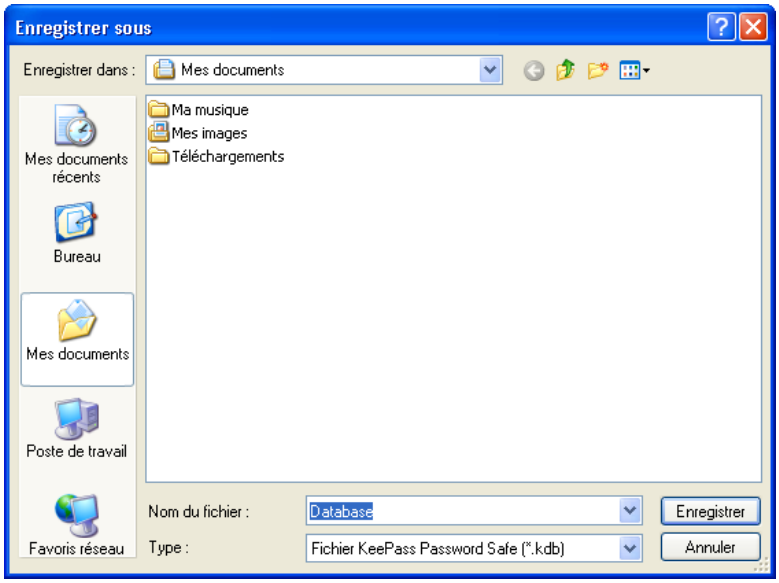


Figure 10: La fenêtre Enregistrer sous

Deuxième étape. **Saisissez** le nom désiré pour votre base de de mots de passe.

Troisième étape. **Cliquez** sur Enregistrer pour sauvegarder votre base de mots de passe.

Astuce: N'oubliez pas l'emplacement et le nom de fichier de votre base de mots de passe! Cela vous sera utile lorsque viendra le temps d'en faire une copie de sauvegarde.

Félicitations! Vous venez de créer et de sauvegarder votre base de mots de passe sécurisée. Vous pouvez désormais commencer à la remplir avec tous vos mots de passe actuels et futurs.

2.2. Comment ajouter une entrée

La fenêtre *Ajouter une entrée* vous permet d'ajouter les détails de vos comptes, vos mots de passe et d'autres renseignements importants à votre base de données. Dans l'exemple qui suit, vous ajouterez des entrées pour sauvegarder des mots de passe et des noms d'utilisateur associés à divers sites Internet et comptes de courriel.

Première étape. **Sélectionnez: Édition > Ajouter une entrée** à partir de la fenêtre *Password Safe* de **KeePass** pour activer la fenêtre Ajouter une entrée, comme suit:

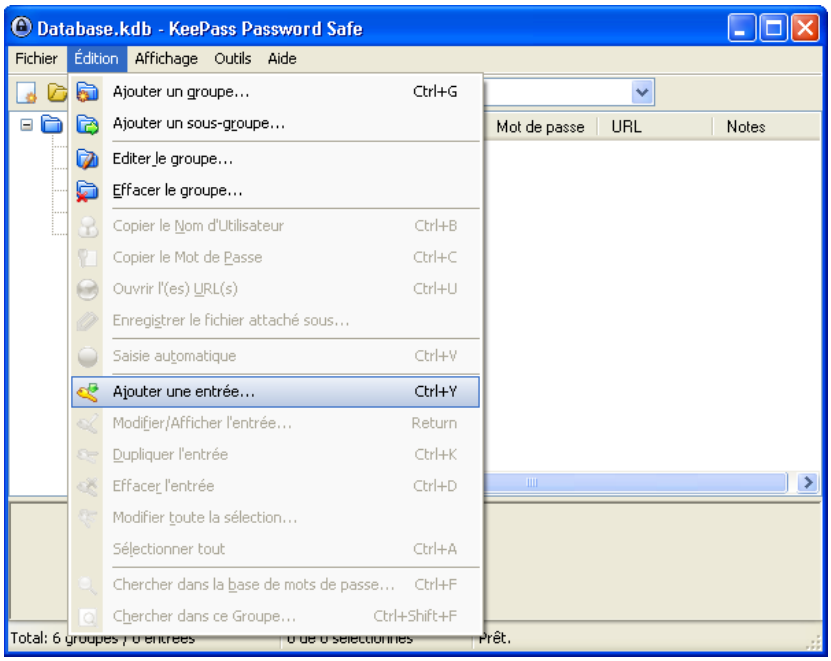


Figure 11: La fenêtre principale de KeePass, avec Édition > Ajouter une entrée sélectionné

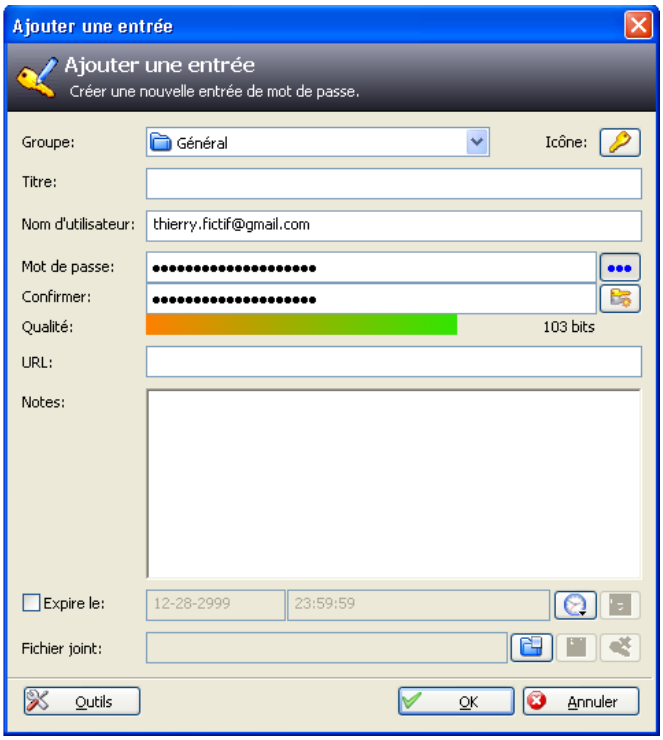


Figure 12: La fenêtre Ajouter une entrée

Commentaire: La fenêtre *Ajouter une entrée* vous présente plusieurs zones à remplir. Aucune de ces zones n'est obligatoire; les renseignements saisis ici servent principalement à faciliter l'utilisation. Ces renseignements pourraient s'avérer utiles dans des situations où vous seriez à la recherche d'une entrée en particulier.

Voici une courte explication pour chacune de ces zones de saisie:

- **Groupe**: **KeePass** vous permet de trier vos mots de passe dans des groupes prédéfinis. Par exemple, Internet est un bon emplacement pour stocker vos mots de passe associés à des comptes d'utilisateur sur des sites Internet. .
- **Titre**: Un titre pour décrire cette entrée de mot de passe. Par exemple: mot de passe Gmail.
- **Nom d'utilisateur**: Le nom d'utilisateur associé à cette entrée de mot de passe. Par exemple: securitybox@gmail.com
- **URL**: Le site Internet associé à cette entrée de mot de passe. Par exemple: https://mail.google.com
- **Mot de passe**: Cette fonctionnalité génère automatiquement un mot de passe aléatoire lorsque la fenêtre Ajouter une entrée est activée. Si vous enregistrez un nouveau compte de courriel, vous pouvez utiliser le mot de passe par défaut inscrit dans cette zone. Vous pouvez également utiliser cette fonction si vous désirez changer votre mot de passe existant pour un nouveau mot de passe généré par **KeePass**. Comme **KeePass** le conservera toujours pour vous, il n'est même pas nécessaire de voir ce mot de passe. Un mot de passe généré aléatoirement est considéré comme fort (c.-à-d. qu'un intrus aura de la difficulté à le deviner ou le déchiffrer).

La génération aléatoire sur demande d'un mot de passe sera expliquée à la prochaine section. Vous pouvez évidemment remplacer le mot de passe par défaut par un mot de passe de votre choix. Par exemple, si vous créez une entrée pour un compte qui existe déjà, il est souhaitable de saisir le mot de passe correspondant (existant) dans cette zone.

- **Confirmer**: La confirmation du mot de passe saisi.

- **Qualité**: Une barre de gradation qui mesure la force du mot de passe selon la longueur et le degré d'aléatoire. Plus la barre est verte, plus le mot de passe choisi est fort.
- **Notes**: C'est dans cette zone que vous saisissez des renseignements généraux concernant le compte ou le site pour lequel vous stockez de l'information. Par exemple : POP3 SSL, pop.gmail.com, Port 995; SMTP TLS, smtp.gmail.com, Port: 465*

Commentaire: Le fait de créer ou modifier les entrées de mot de passe dans **KeePass** ne change pas réellement vos mots de passe! Considérez **KeePass** comme un livre d'adresses sécurisé où sont stockés vos mots de passe. Vous n'y trouvez que ce que vous y consignez, rien de plus.

Si vous sélectionnez *Internet* dans le menu défilant *Groupe*, votre entrée de mot de passe ressemblera peut-être à ceci :

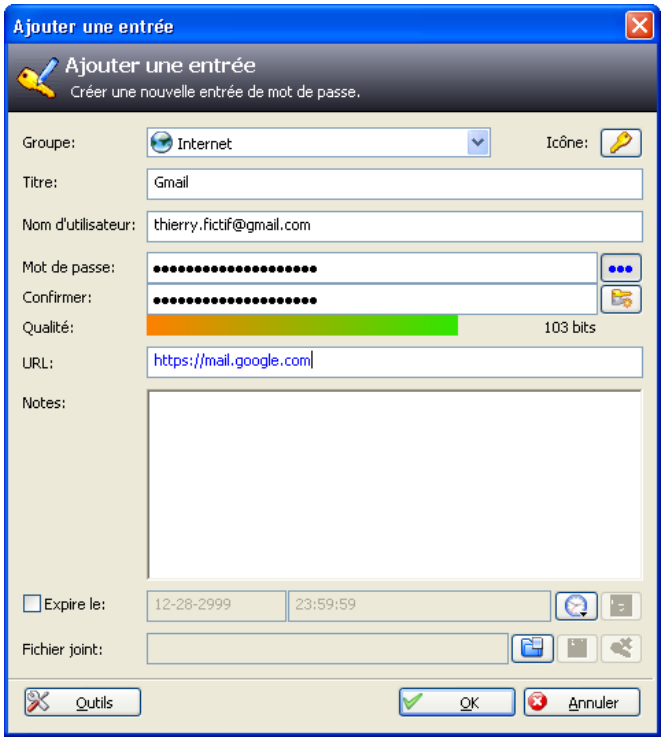


Figure 13: La fenêtre Ajouter une entrée remplie

Deuxième étape. **Cliquez** sur pour sauvegarder cette entrée.

*Votre mot de passe se trouve désormais dans le groupe **Internet**.*

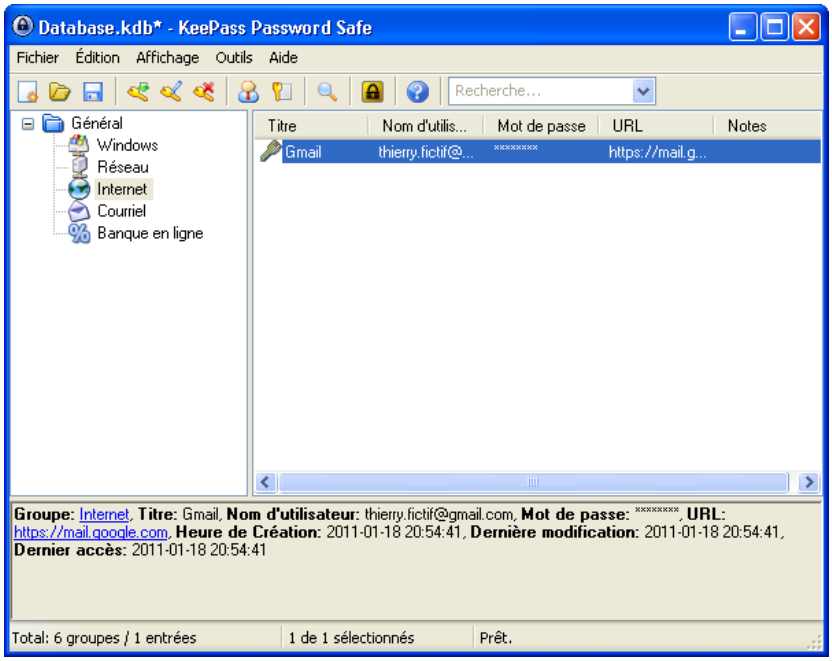


Figure 14: La fenêtre principale de KeePass Password Safe

Commentaire: Le panneau d'affichage au bas de cette fenêtre montre les renseignements inclus dans l'entrée sélectionnée. Cela comprend la création, l'édition et la date d'expiration, ainsi que les notes enregistrées dans cette entrée. Le mot de passe n'y est pas révélé.

- **Expire le**: Cochez cette option pour activer les zones de texte où vous pouvez spécifier une date limite de validité. Ce faisant, vous pouvez ajouter une note qui vous rappellera de changer votre mot de passe à date fixe (tous les trois mois, par exemple). Lorsqu'un mot de passe aura dépassé sa date limite de validité, une petite croix rouge apparaîtra à côté

de son nom, tel qu'illustré dans l'exemple ci-dessous:

NetSecuredb.kdb* - KeePass Password Safe
File Edit View Tools Help
Search...
Internet
Windows
Network
Internet
eMail
Homebanking
Backup
Title User Name Password URL Notes
Gmail securitybox.org ******** https://mail.g... Mail Server s...
Group: Internet, Title: Gmail, User Name: securitybox.org, Password: ********, URL: https://mail.google.com, Creation Time: 12/11/2010 08:31:37, Last Modification: 12/11/2010 08:35:31, Last Access: 12/11/2010 08:35:31, Expires: 12/11/2010 08:35:00
Mail Server settings: POP3 SSL, pop.gmail.com, Port 995; SMTP TLS, smtp.gmail.com, Port: 465
Total: 7 groups / 3 entries
1 of 1 selected
Ready.

Figure 15: Un exemple de clé expirée

2.3 Comment éditer une entrée

Il est possible d'éditer une entrée existante dans **KeePass**, et ce, en tout temps. Vous pouvez changer votre mot de passe (il est indiqué, pour des raisons de sécurité, de changer un mot de passe régulièrement tous les trois à six mois), ou modifier les autres détails inclus dans l'entrée du mot de passe.

Pour éditer une entrée, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez** le bon *Groupe* dans la colonne de gauche pour activer les entrées qui y sont associées.

Deuxième étape. **Sélectionnez** l'entrée pertinente, puis **cliquez à droite** sur l'entrée sélectionnée pour activer la fenêtre ci-dessous :

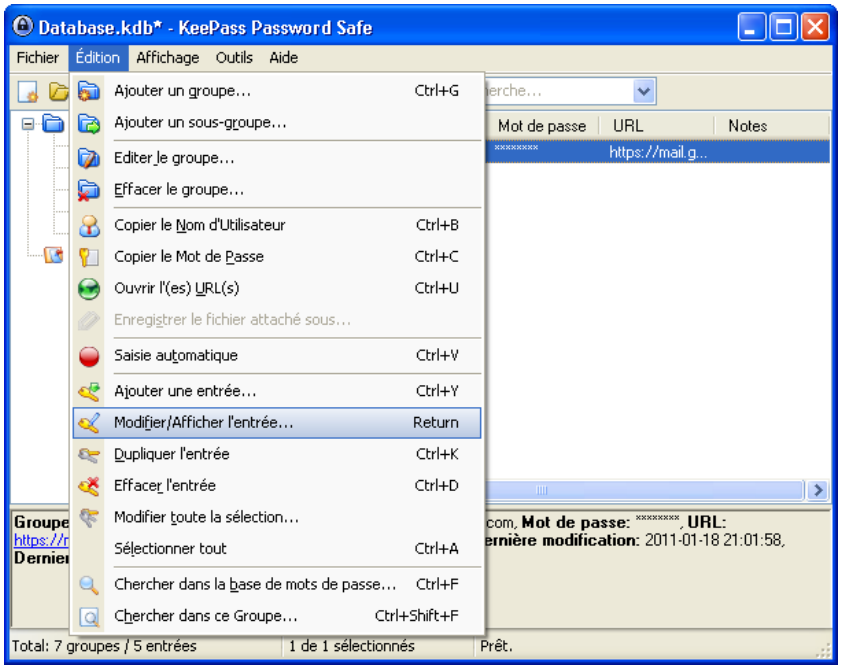
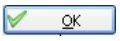

Database.kdb* - KeePass Password Safe
Fichier Édition Affichage Outils Aide
Ajouter un groupe... Ctrl+G
Ajouter un sous-groupe...
Editer le groupe...
Effacer le groupe...
Copier le Nom d'Utilisateur Ctrl+B
Copier le Mot de Passe Ctrl+C
Ouvrir l'(es) URL(s) Ctrl+U
Enregistrer le fichier attaché sous...
Saisie automatique Ctrl+V
Ajouter une entrée... Ctrl+Y
Modifier/Afficher l'entrée... Return
Dupliquer l'entrée Ctrl+K
Effacer l'entrée Ctrl+D
Modifier toute la sélection...
Sélectionner tout Ctrl+A
Chercher dans la base de mots de passe... Ctrl+F
Chercher dans ce Groupe... Ctrl+Shift+F
Mot de passe URL Notes
https://mail.g...
Total: 7 groupes / 5 entrées
1 de 1 sélectionnés
Prêt.

Figure 16: La fenêtre principale de KeePass Password Safe affichant le menu Édition

Troisième. **Cliquez** sur  pour sauvegarder tout changement, y compris le mot de passe.

Pour changer un mot de passe existant (que vous aviez préalablement créé vous-même) pour un nouveau mot de passe généré aléatoirement par KeePass, veuillez lire la section suivante.

2.4 Comment générer des mots de passe aléatoirement

De longs mots de passe aléatoires sont considérés comme forts dans le monde de la sécurité informatique. Leur nature aléatoire est fondée sur des principes mathématiques et il est pratiquement impossible pour un intrus de les deviner. **KeePass** fournit un *générateur de mot de passe* pour vous assister dans ce processus. Comme vous l'avez vu ci-dessus, un mot de passe aléatoire est automatiquement généré lorsque vous créez une nouvelle entrée. Cette section vous montrera comment en générer un par vous-même.

Commentaire: Le *générateur de mot de passe* peut être activé depuis les fenêtres *Ajouter une entrée* et *Modifier/Afficher l'entrée*. Sinon, **sélectionnez: Outils > Générateur de mots de passe**.

Première étape. **Cliquez** sur depuis la fenêtre *Ajouter une entrée* ou la fenêtre *Modifier/Afficher l'entrée*, pour afficher la fenêtre *Générateur de mots de passe* illustrée ci-dessous :

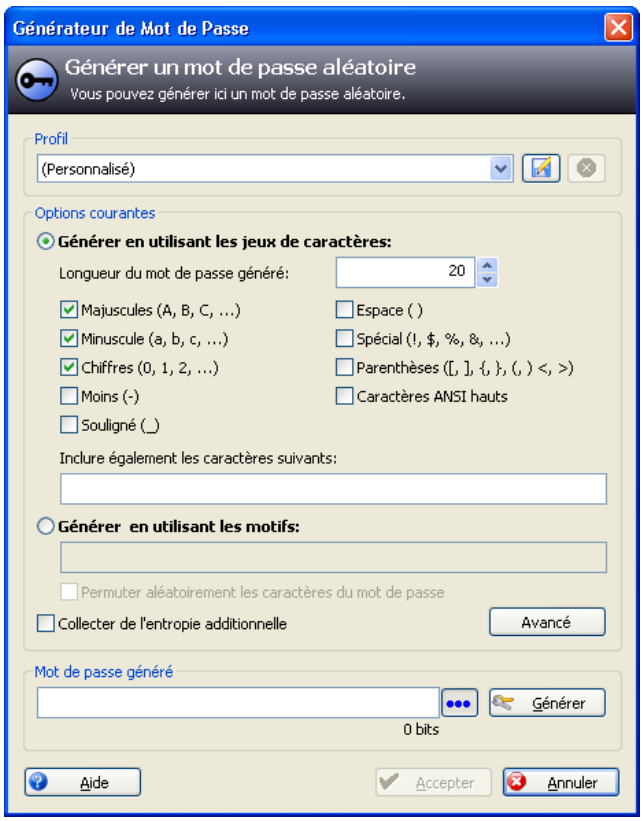


Figure 17: La fenêtre Générateur de mots de passe

La fenêtre *Générateur de mots de passe* présente plusieurs options pour générer un mot de passe. Vous pouvez préciser la longueur du mot de passe souhaité, les jeux de caractères utilisés pour le créer, et bien plus. Pour les fins de cet exemple, conservons les paramètres par défaut qui nous sont présentés. Cela signifie que le mot de passe généré comportera 20 caractères et sera composé de lettres majuscules et minuscules, ainsi que de chiffres.

Deuxième étape. **Cliquez** sur

pour entamer le processus. Lorsque celui-ci sera terminé, **KeePass** vous présentera le mot de passe généré.

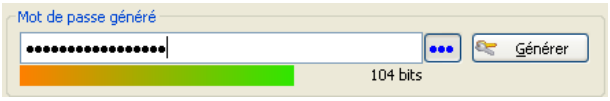
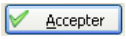


Figure 18: La rubrique Mot de passe généré de KeePass

Commentaire: Vous pouvez visionner le mot de passe généré en **cliquant** . Cependant, cela comporte un risque de sécurité, comme nous l'avons déjà mentionné. Au fond, vous n'aurez jamais vraiment besoin de voir le mot de passe généré. Nous y reviendrons à la section **3.0 Comment utiliser les mots de passe** [57].

Troisième étape. **Cliquez** sur 

pour accepter le mot de passe et retourner à la fenêtre Ajouter une entrée illustrée ci-dessous:

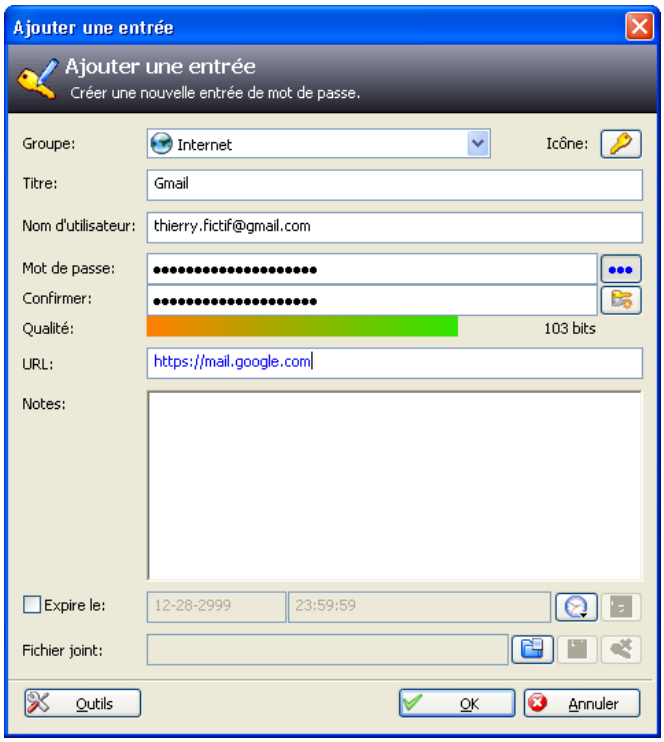


Figure 19: La fenêtre Ajouter une entrée

Quatrième étape. **Cliquez** sur pour sauvegarder cette entrée.

Cinquième étape. **Sélectionnez: Fichier > Enregistrer** pour sauvegarder la base de données ainsi mise à jour.

2.5 Comment fermer, réduire ou restaurer KeePass

Vous pouvez réduire ou fermer le logiciel **KeePass** en tout temps. Lorsque vous souhaiterez rouvrir ou restaurer le programme, une invite vous demandera de saisir de nouveau votre mot de *passe principal*.

KeePass se réduit automatiquement et cet icône s'affiche dans votre barre de tâches système (dans le coin inférieur droit de votre écran).

KeePass vous permet également de verrouiller le programme en suivant les étapes décrites ci-dessous:

Première étape. **Sélectionnez: Fichier> Verrouiller l'espace de travail** pour afficher la fenêtre suivante:

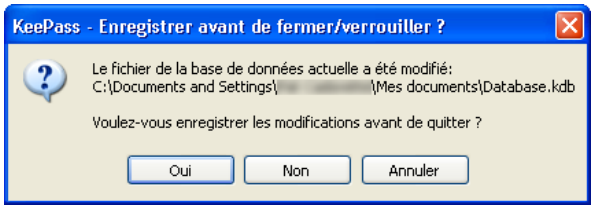
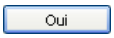

KeePass - Enregistrer avant de fermer/verrouiller ?
Le fichier de la base de données actuelle a été modifié:
C:\Documents and Settings\ \Mes documents\Database.kdb
Voulez-vous enregistrer les modifications avant de quitter ?
Oui
Non
Annuler

Figure 20: La fenêtre Enregistrer avant de fermer/verrouiller de KeePass

Deuxième étape. **Cliquez** sur  pour sauvegarder l'information et désactiver la console **KeePass**, qui devrait maintenant ressembler à la *figure 2*. Cet icone apparaît désormais dans votre *barre de tâches système*:

Première étape. **Double-cliquer** sur cet icone pour restaurer **KeePass** à la grandeur normale et afficher la fenêtre suivante:

Figure 21: La fenêtre Ouvrir base de données Database.kdb

Troisième étape. **Saisissez** votre *Mot de passe principal* pour ouvrir **KeePass**.

Pour fermer **KeePass**:

Première étape. **Sélectionnez: Fichier > Quitter** pour fermer complètement le programme **KeePass**.

Si des changements ont été apportés à la banque de mots de passe mais n'ont pas été sauvegardés, **KeePass** vous invitera à enregistrer la sauvegarde.

2.6 Comment créer une copie de sauvegarde de la base de mots de passe

Le fichier de la base de mots de passe KeePass qui se trouve sur votre ordinateur est désigné par l'extension de fichier .kdb. Vous pouvez copier ce fichier sur une clé USB. Personne d'autre que vous ne sera en mesure d'ouvrir la base de donnée, à moins de connaître le mot de passe principal.

Première étape. **Sélectionnez: Fichier > Enregistrez sous** depuis la fenêtre principale, puis sauvegardez une copie de la base de données à un autre emplacement.

Il est possible d'exécuter le programme **KeePass** depuis une clé USB. Veuillez consulter le guide pratique **KeePass Portable** [58].

2.7 Comment réinitialiser votre mot de passe principal

Vous pouvez changer votre *mot de passe principal* en tout temps. Pour ce faire, il faut d'abord ouvrir la banque de mots de passe.

Première étape. **Sélectionnez: Fichier > Modifier la clé maître**

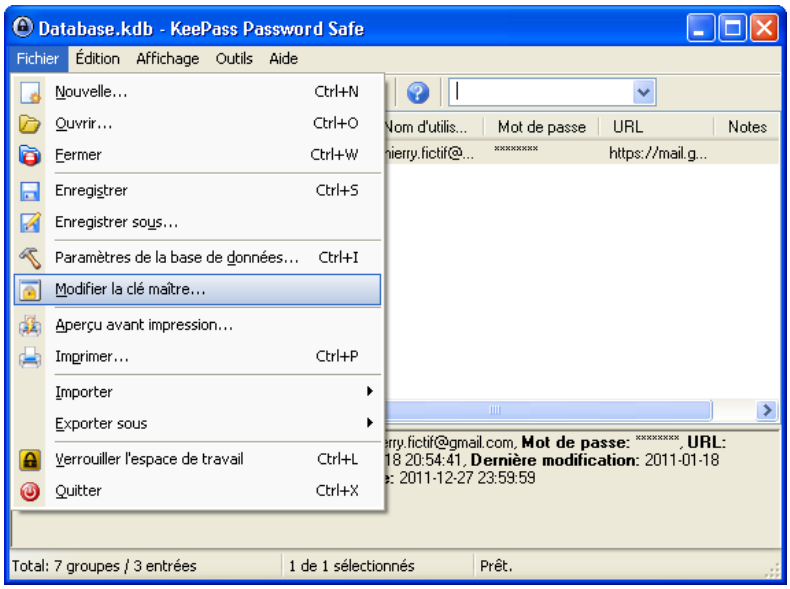


Figure 22: Le menu fichier avec l'option Modifier la clé maître sélectionnée

Deuxième étape. **Saisissez** deux fois votre nouveau *Mot de passe principal*.

Figure 23: La fenêtre Modifier la clé composite principale

Comment utiliser les mots de passe

3.0 Comment utiliser les mots de passe

Puisqu'un mot de passe sécurisé est difficile à mémoriser, **KeePass** vous permet de le copier depuis la base de données et le coller directement dans le compte ou le site Internet qui le requiert. Pour plus de sécurité, un mot de passe copié ne restera

pas plus de 10 secondes dans le presse-papiers, alors il est conseillé d'avoir déjà ouvert le compte ou le site Internet pour que vous puissiez y copier rapidement votre mot de passe.

Première étape. **Cliquez à droite** sur l'entrée de mot de passe appropriée pour activer le menu contextuel.

Deuxième étape. **Sélectionnez : Copier le Mot de passe dans le Presse-Papiers** comme suit:

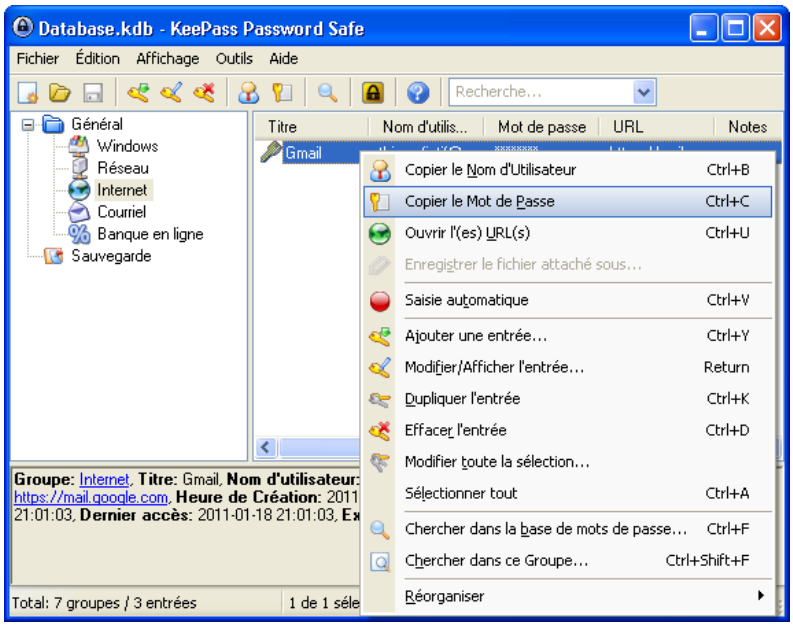


Figure 1: La fenêtre de KeePass Password Safe

Troisième étape. Rendez-vous dans le compte ou sur le site pertinent et **collez** le mot de passe dans la zone appropriée :

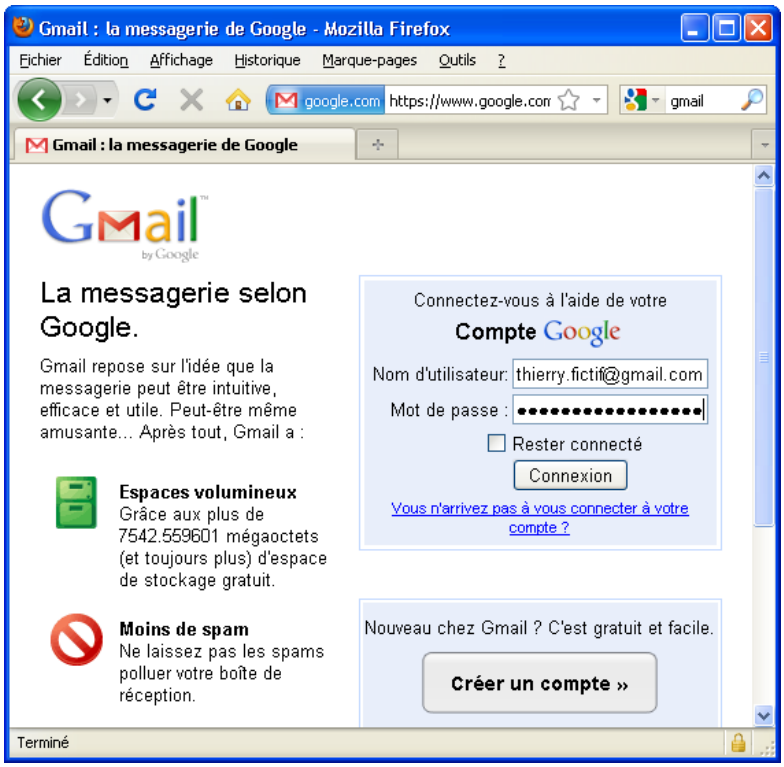

Gmail : la messagerie de Google - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
google.com https://www.google.com
gmail
Gmail : la messagerie de Google
Gmail by Google
La messagerie selon Google.
Gmail repose sur l'idée que la messagerie peut être intuitive, efficace et utile. Peut-être même amusante... Après tout, Gmail a :
Espaces volumineux
Grâce aux plus de 7542.559601 mégaoctets (et toujours plus) d'espace de stockage gratuit.
Moins de spam
Ne laissez pas les spams polluer votre boîte de réception.
Connectez-vous à l'aide de votre
Compte Google
Nom d'utilisateur: thierry.fictif@gmail.com
Mot de passe :
Rester connecté
Connexion
Vous n'arrivez pas à vous connecter à votre compte ?
Nouveau chez Gmail ? C'est gratuit et facile.
Créer un compte »
Terminé

Figure 2: Un compte de courriel Gmail affichant un mot de passe copié-collé

Astuce: Pour copier, coller et changer de fenêtre efficacement, utilisez les raccourcis de clavier. **Pressez et maintenez enfoncée** la touche **Ctrl**, puis appuyez sur la touche *C* pour copier un mot de passe. **Pressez et maintenez enfoncée** la touche **Ctrl**, puis appuyez sur la touche *V* pour coller ce mot de passe. **Pressez et maintenez enfoncée** la touche *Alt*, puis appuyez sur la touche *Tab* pour naviguer entre les programmes et les fenêtres ouvertes.

Commentaire: En utilisant constamment **KeePass**, vous n'avez pas besoin de voir votre mot de passe, ni même de le connaître. La fonction copier/coller suffit à transférer le mot de passe de la base de données à la fenêtre appropriée. Si vous utilisez la fonction *Générateur de mot de passe* et transférez ensuite ce mot de passe dans un nouveau compte de courriel, vous utiliserez un mot de passe que vous n'aurez en fait jamais vu. Et ça fonctionne!

Faq et questions récapitulatives

4.0 Faq et questions récapitulatives

KeePass KeePass semble être un programme facile à utiliser pour Nikolai et Elena. Le seul aspect qui leur paraît plus difficile est de prendre l'habitude de créer de nouveaux mots de passe avec **KeePass**. Elena a du mal à se faire à l'idée qu'elle ne verra jamais plus de mots de passe, mais c'est définitivement plus facile que de devoir s'en rappeler!

Q: *Nikolai, j'ai été surprise de constater à quel point il est facile de se servir de **KeePass**. Par contre, si jamais par malheur j'oubliais mon mot de passe principal, y aurai-t-il une façon d'accéder à **KeePass** pour récupérer ma banque de mots de passe?*

A: *Elle est facile celle-là, Elena! Non. Désolé, il n'y a rien à faire dans cette situation. Mais pour prendre les choses du bon côté, au moins, personne d'autre ne sera en mesure d'accéder à ta banque de mots de passe! Pour empêcher que cela ne se produise, tu peux toujours employer l'une ou l'autre des méthodes pour se souvenir d'un mot de passe qui sont suggérées au chapitre **3. Créer et sauvegarder des mots de passe sûrs** [53] du livret pratique*

Q: *Et si je désinstalle **KeePass**, qu'adviendra-t-il de mes mots de passe?*

A: *Le programme sera supprimé de ton ordinateur, mais ta base de données (stockée dans le fichier .kdb) s'y trouvera toujours. Tu pourras ouvrir ce fichier en tout temps si tu réinstalles **KeePass** plus tard.*

Q: *Je crois que j'ai supprimé le fichier de la base de données par erreur!*

A: *J'espère que tu avais fait une copie de sauvegarde! Aussi, assure-toi que tu n'as pas simplement oublié l'emplacement de ton fichier. Exécute une recherche sur ton ordinateur pour trouver un fichier comprenant l'extension .kdb. Si tu l'as effectivement supprimé, jette un coup d'œil au Guide pratique **Recuva** [59]. Cela pourrait t'aider à retrouver ton fichier.*

4.1 Questions récapitulatives

- Qu'est-ce qui constitue un mot de passe fort?
- Comment puis-je modifier une entrée de mot de passe existante dans **KeePass**?
- Comment puis-je générer un mot de passe de 30 caractères dans **KeePass**?

TrueCrypt - stockage de fichiers sécurisé

Short Description:

TrueCrypt protège vos données en empêchant quiconque ne dispose pas du bon mot de passe d'y accéder. C'est en quelque sorte un «coffre-fort» électronique où vous rangez vos fichiers en sûreté.

Online Installation Instructions:

Pour télécharger TrueCrypt

- *Lisez la courte introduction aux **Guides pratiques** [1]*
- ***Cliquez** sur l'icone **TrueCrypt** ci-dessous pour ouvrir la page de téléchargement **www.truecrypt.org/downloads***
- *Sous la section **Latest Stable Version - Windows**, **cliquez** sur le bouton **Download***
- *Sauvegardez le fichier d'installation sur votre ordinateur à un emplacement de votre choix, puis cliquez dessus pour lancer l'installation.*
- *Lisez attentivement les consignes d'installation avant de continuer*
- *Vous pouvez supprimer l'exécutable après l'installation.*

TrueCrypt:

[60]

Pour utiliser TrueCrypt en français

- Installez KeePass en suivant les consignes indiquées à la section **2.0 Comment installer TrueCrypt** [61]
- Rendez-vous à la **page web des traductions de TrueCrypt** [62]
- Localisez le fichier .zip de traduction française **langpack-fr-0.1.0-for-truecrypt-7.0a** et sauvegardez-le à un emplacement de votre choix.
- Décompactez le fichier .zip, et copiez le fichier *Language.fr.xml* dans le répertoire où **TrueCrypt** est installé (habituellement C:/Program Files/TrueCrypt).
- Démarrez **TrueCrypt**. Le logiciel devrait s'ouvrir en français. Sinon, allez au menu *Settings* > *Language* et **sélectionnez** *Français*.

Site Internet

www.truecrypt.org [63]

Configuration requise

- Windows 2000/XP/2003/Vista/7
- Les droits d'administration sont nécessaires pour installer le logiciel et créer des volumes chiffrés, mais pas pour accéder aux volumes existants.

Version utilisée pour rédiger ce guide

- 7.0a

Licence

- FLOSS (Free/Libre & Open Source Software)

Lecture préalable

- Livret pratique Security in-a-box, chapitre **4. Protéger les données sensibles stockées sur votre ordinateur** [64]

Niveau

- (Volumes Standards): 1 : Débutant, 2 : Moyen, **3 : Intermédiaire**, 4 : Expérimenté, 5 : Avancé
- (Volumes cachés): 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, **4 : Expérimenté**, 5 : Avancé

Temps d'apprentissage:

- (Volumes Standards): 30 minutes
- (Volumes cachés): 30 minutes

**Ce que vous apportera l'utilisation de cet outil **:

- La capacité de protéger efficacement vos fichiers de toute intrusion et de tout accès non autorisé.
- La capacité de stocker facilement des copies de sauvegarde de vos fichiers importants, et ce, de façon sécurisée.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Commentaire: Nous recommandons fortement **TrueCrypt** pour **GNU Linux** et **Mac OS**.

Plusieurs distributions de **GNU Linux**, par exemple **Ubuntu** [65], supportent le chiffrement/déchiffrement à la volée du disque au complet. Vous pouvez choisir d'utiliser cette fonction standard à l'installation du système. Vous pouvez également ajouter la fonction de chiffrement à votre système **Linux** en utilisant l'intégration de **dm-crypt** [66] et **cryptsetup et LUKS** [67]. Une autre approche consiste à utiliser **ScramDisk pour Linux SD4L** [68], un programme gratuit et de source libre de chiffrement/déchiffrement à la volée.

Pour **Mac OS**, vous pouvez utiliser **FileVault**, qui est intégré au système d'exploitation, pour chiffrer et déchiffrer à la volée le contenu de votre répertoire *Home* et tous ses dossiers. On trouve également un programme gratuit et de source libre **Encrypt This** [69]. Ce programme permet de chiffrer des fichiers choisis dans une image de disque .DMG.

Il existe plusieurs programmes de chiffrement pour **Microsoft Windows**. Nous recommandons ceux-ci:

- **FREE CompuSec** [70] est un programme gratuit, propriétaire, de chiffrement/déchiffrement à la volée. Il peut, chiffrer un disque dur, une clé USB ou un CD en partie ou au complet. Le module **DataCrypt** de **CompuSec** peut être utilisé pour chiffrer des fichiers individuels.
- **CryptoExpert 2009 Lite** [71] est un programme gratuit, propriétaire, de chiffrement/déchiffrement à la volée qui crée des volumes chiffrés, à la manière de **TrueCrypt**.
- **AxCrypt** [72] est un programme gratuit et de source libre qui permet de chiffrer des fichiers individuels.
- **Steganos LockNote** [73] est un programme gratuit et de source libre. Il peut être utilisé pour chiffrer et déchiffrer n'importe quel texte. Le texte sera stocké dans l'application **LockNote**: Le mécanisme qui permet de chiffrer ou de déchiffrer une note est incorporé au fichier. **LockNote** est portable et aucune installation n'est requise.

1.1 À propos de cet outil

TrueCrypt protégera vos données en les verrouillant derrière un mot de passe que vous créerez vous-même. Attention : Si vous oubliez le mot de passe, vous perdrez l'accès à vos données! **TrueCrypt** utilise un processus de chiffrement pour protéger vos fichiers (veuillez vous assurer que le chiffrement est légal dans votre pays!). Au lieu de chiffrer les fichiers existants, **TrueCrypt** crée une section protégée sur votre ordinateur, un *volume* chiffré, où vous pouvez ensuite stocker des fichiers de façon sécurisée.

TrueCrypt offre la possibilité de créer un volume standard ou un volume caché. D'une manière ou d'une autre, vos fichiers resteront confidentiels, mais un volume caché vous permet de dissimuler vos données les plus importantes derrière des données moins délicates, ce qui les protège même lorsque vous êtes forcé à ouvrir votre volume **TrueCrypt** standard. Le présent guide explique comment fonctionnent les deux types de volume.

Comment installer TrueCrypt et créer des volumes standards

Sommaire des sections de cette page:

- **2.0 Comment installer TrueCrypt**
- **2.1 À propos de TrueCrypt**
- **2.2 Comment créer un volume standard**
- **2.3 Comment créer un volume standard sur une clé USB**
- **2.4 Comment créer un volume standard (suite)**

2.0 Comment installer TrueCrypt

Première étape. **Double-cliquez** TrueCrypt Setup 7.0a; si la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, **cliquez** sur Run pour afficher la fenêtre **TrueCrypt** *License*.

Deuxième étape. **Cochez** l'option *I accept and agree to be bound by the license terms* pour activer le bouton *Accept*; **cliquez** sur Exécuter pour afficher la fenêtre suivante:

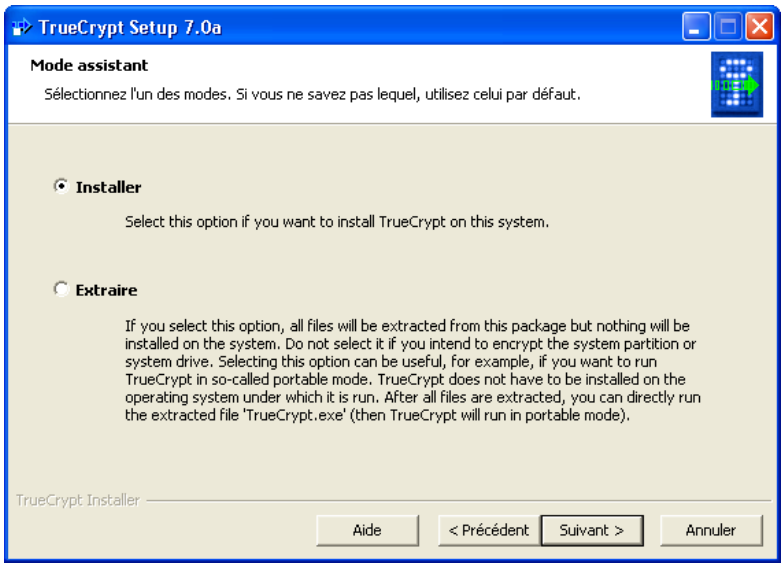

TrueCrypt Setup 7.0a
Mode assistant
Sélectionnez l'un des modes. Si vous ne savez pas lequel, utilisez celui par défaut.
Installer
Select this option if you want to install TrueCrypt on this system.
Extraire
If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).
TrueCrypt Installer
Aide
< Précédent
Suivant >
Annuler

Figure 1: Le Mode assistant en mode d'installation par défaut

- Le mode *Installer*: Cette option est pour les utilisateurs qui ne souhaitent pas cacher le fait qu'ils utilisent **TrueCrypt** sur leur ordinateur.
- Le mode *Extraire*: Cette option est pour les utilisateurs qui souhaitent transporter une version portable de **TrueCrypt** sur une clé USB et qui ne souhaitent pas installer **TrueCrypt** sur leur ordinateur.

Commentaire: Certaines options (par exemple, le chiffrement de partitions entières et de disques entiers) ne fonctionneront pas si **TrueCrypt** est extrait mais non installé.

Commentaire: Même si le mode *Installer* par défaut est recommandé ici, vous voudrez peut-être utiliser la version portable de **TrueCrypt** ultérieurement. Pour en savoir plus sur le mode **TrueCrypt Traveller**, veuillez consulter le chapitre **TrueCrypt mode Traveler** [74].

Troisième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

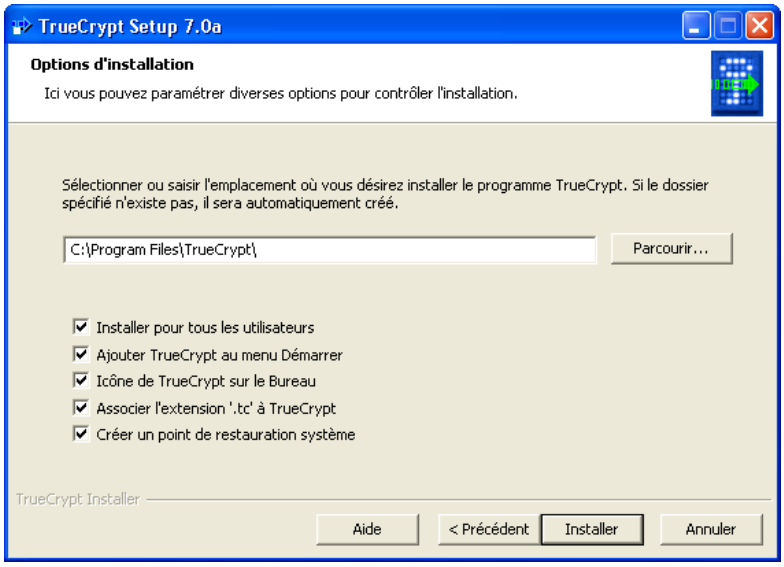

TrueCrypt Setup 7.0a
Options d'installation
Ici vous pouvez paramétrer diverses options pour contrôler l'installation.
Sélectionner ou saisir l'emplacement où vous désirez installer le programme TrueCrypt. Si le dossier spécifié n'existe pas, il sera automatiquement créé.
C:\Program Files\TrueCrypt\
Parcourir...
Installer pour tous les utilisateurs
Ajouter TrueCrypt au menu Démarrer
Icône de TrueCrypt sur le Bureau
Associer l'extension '.tc' à TrueCrypt
Créer un point de restauration système
TrueCrypt Installer
Aide
< Précédent
Installer
Annuler

Figure 2: La fenêtre Options d'installation

Quatrième étape. **Cliquez** sur Installer pour afficher la fenêtre *Installation en cours* et lancer l'installation de **TrueCrypt** sur votre système.

Cinquième étape. **Cliquez** sur OK pour afficher la fenêtre suivante:

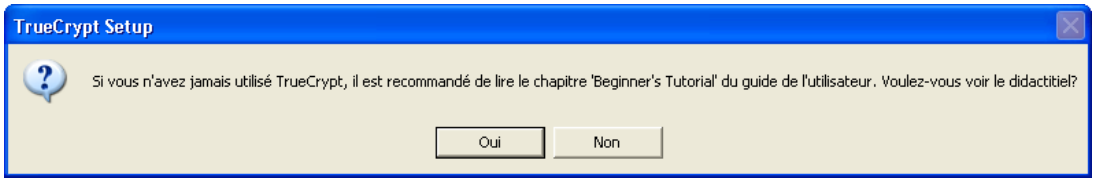

TrueCrypt Setup
Si vous n'avez jamais utilisé TrueCrypt, il est recommandé de lire le chapitre 'Beginner's Tutorial' du guide de l'utilisateur. Voulez-vous voir le didactitiel?
Oui
Non

Figure 3: La boîte de dialogue de confirmation de l'installation de TrueCrypt

Sixième étape. **Cliquez** sur Oui pour ouvrir le site Internet de **TrueCrypt** et finaliser l'installation de *TrueCrypt**, puis **cliquez** sur Terminer.

Commentaire: Il est recommandé à tous les utilisateurs de consulter la documentation d'aide fournie par **TrueCrypt**.

2.1 À propos de TrueCrypt

TrueCrypt est conçu pour sécuriser vos fichiers en bloquant l'accès à quiconque ne dispose pas du mot de passe nécessaire. Le logiciel fonctionne un peu comme un "coffre-fort" électronique en vous permettant de verrouiller vos fichiers de telle sorte que seule une personne disposant du bon mot de passe puisse y accéder. **TrueCrypt** vous permet de créer des *volumes*, ou des sections de votre ordinateur où vous pouvez stocker des fichiers de façon sécurisée. Lorsque vous créez des données dans ces volumes, ou lorsque vous y transférez des données, TrueCrypt chiffre automatiquement cette information. Lorsque vous ouvrez ou déplacez ces fichiers, le programme les déchiffre automatiquement. Ce processus s'appelle chiffrage/déchiffrage *à la volée*.

2.2 Comment créer un volume standard

TrueCrypt vous donne le choix de créer deux types de volumes: *caché* et *standard*. Dans cette section section, nous verrons comment créer un *volume standard* pour y stocker vos fichiers.

Pour commencer à utiliser **TrueCrypt** en créant un *volume standard*, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** ou **Sélectionnez Démarrer > Programmes > TrueCrypt > TrueCrypt** pour ouvrir **TrueCrypt**.

Deuxième étape. **Sélectionnez** un lecteur dans la liste du panneau principal **TrueCrypt** illustré ci-dessous:

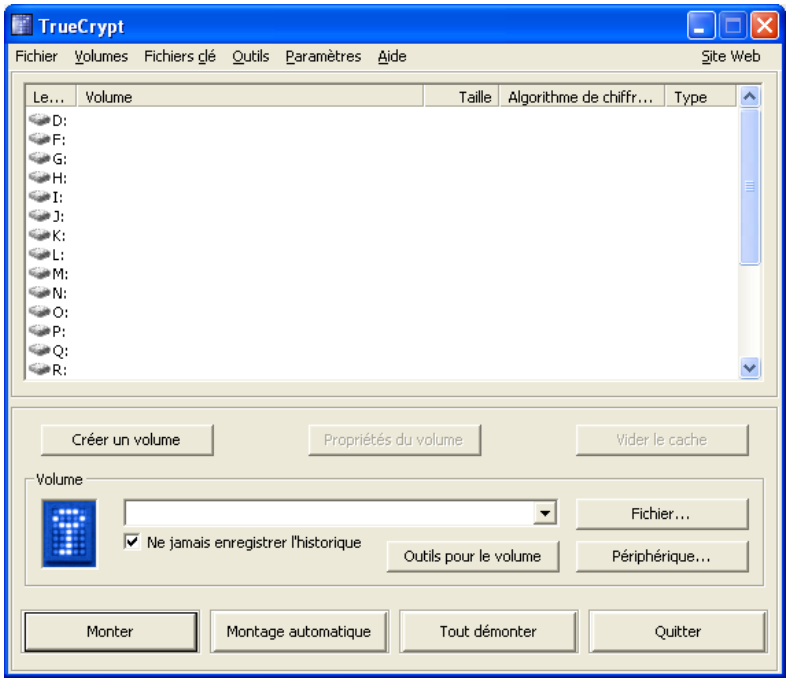


Figure 4: La console TrueCrypt

Troisième étape. **Cliquez** sur Créer un volume pour activer l'*Assistant de création de volume TrueCrypt*, illustré ci-dessous:

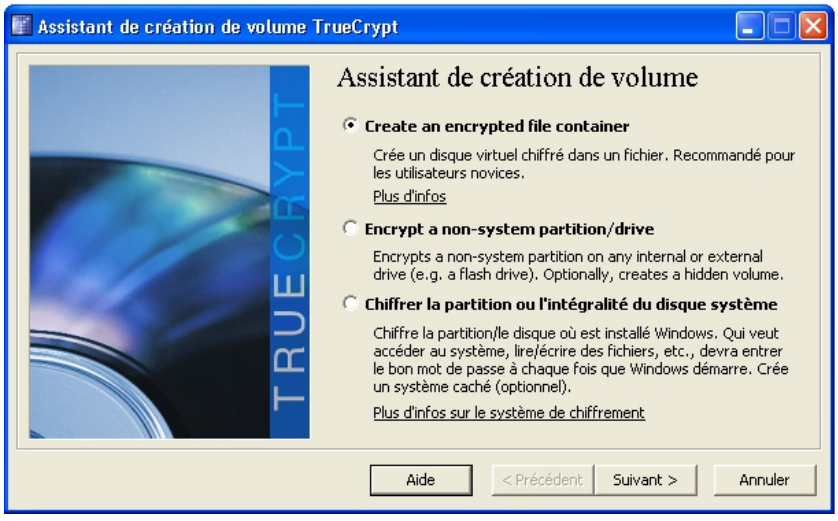

Assistant de création de volume TrueCrypt
Assistant de création de volume
TRUECRYPT
Create an encrypted file container
Crée un disque virtuel chiffré dans un fichier. Recommandé pour les utilisateurs novices.
Plus d'infos
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Chiffrer la partition ou l'intégralité du disque système
Chiffre la partition/le disque où est installé Windows. Qui veut accéder au système, lire/écrire des fichiers, etc., devra entrer le bon mot de passe à chaque fois que Windows démarre. Crée un système caché (optionnel).
Plus d'infos sur le système de chiffrement
Aide
< Précédent
Suivant >
Annuler

Figure 5: L'Assistant de création de volume TrueCrypt

La *figure 5* vous présente trois options pour créer un *volume standard*. Dans ce chapitre, nous aborderons la *Création d'un conteneur chiffré* (*Create an encrypted file container*). Veuillez consulter la documentation de **TrueCrypt** [75] pour obtenir les

descriptions des deux autres options.

Quatrième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

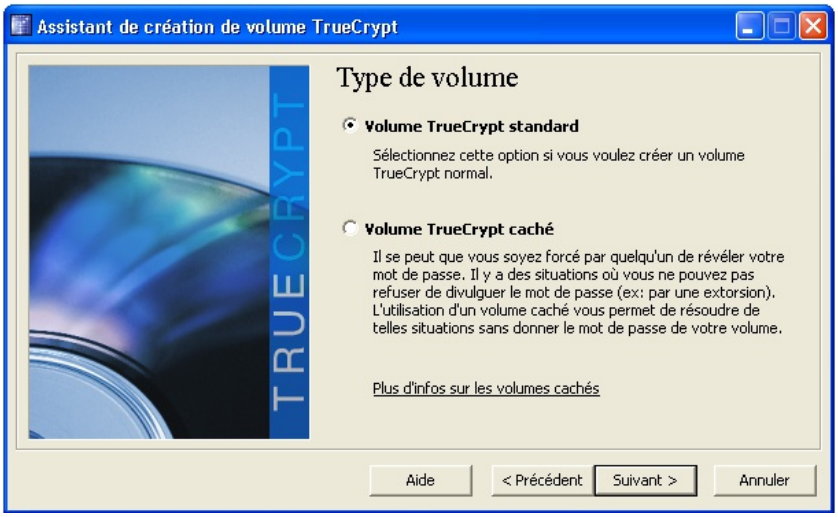

Assistant de création de volume TrueCrypt
Type de volume
Volume TrueCrypt standard
Sélectionnez cette option si vous voulez créer un volume TrueCrypt normal.
Volume TrueCrypt caché
Il se peut que vous soyez forcé par quelqu'un de révéler votre mot de passe. Il y a des situations où vous ne pouvez pas refuser de divulguer le mot de passe (ex: par une extorsion). L'utilisation d'un volume caché vous permet de résoudre de telles situations sans donner le mot de passe de votre volume.
Plus d'infos sur les volumes cachés
Aide
< Précédent
Suivant >
Annuler
TRUECRYPT

Figure 6: La fenêtre Type de volume

La fenêtre *Assistant de création de volume TrueCrypt - Type de volume* offre le choix entre un *volume standard* et un *volume caché*.

Important: Voir la section **Volumes cachés** [76] du présent guide pour plus d'information sur la création d'un *volume caché*.

Cinquième étape. **Cochez** l'option *Volume TrueCrypt Standard*.

Sixième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

Assistant de création de volume TrueCrypt
Emplacement du volume
Fichier...
Ne jamais enregistrer l'historique
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
Aide
< Précédent
Suivant >
Annuler
TRUECRYPT

Figure 7: L'Assistant de création de volume TrueCrypt affichant le panneau Emplacement du volume

Vous pouvez déterminer où vous aimeriez stocker votre *volume standard* dans la fenêtre de l'*Assistant de création de volume - Emplacement du volume*. Ce fichier peut être stocké comme n'importe quel autre type de fichier

Septième étape. **Saisissez** le nom du fichier dans la zone de texte ou **cliquez** sur Fichier... pour afficher la fenêtre suivante:

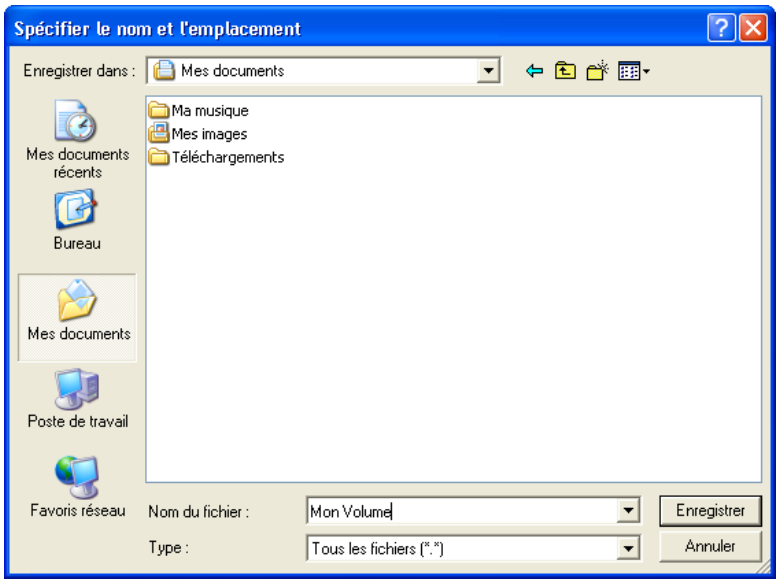


Figure 8: La fenêtre Spécifier le nom et l'emplacement

Commentaire: Un volume **TrueCrypt** est contenu à l'intérieur d'un fichier normal. Cela signifie qu'il peut être déplacé, copié et même supprimé! Il est donc très important de se rappeler le nom et l'emplacement du fichier. Cependant, vous devez choisir un nouveau nom de fichier pour le volume que vous créez (veuillez également consulter la section 2.3 Comment créer un volume standard sur une clé USB). Pour les fins de cet exercice, nous créerons notre *volume standard* dans le répertoire *Mes documents*, et nous nommerons le fichier *Mon volume* (voir Figure 8, ci-dessus).

Astuce: Vous pouvez utiliser n'importe quel nom de fichier et type d'extension. Par exemple, vous pouvez nommer votre volume standard *recettes.doc* pour lui donner l'apparence d'un document *Word*, ou *vacances.mpeg* pour lui donner l'apparence d'un d'un fichier vidéo. C'est un moyen par lequel vous pouvez dissimuler l'existence d'un volume standard.

Huitième étape. **Cliquez** sur Save pour fermer la fenêtre *Spécifier le nom et l'emplacement* et revenir à l'*Assistant de création de volume*:

Figure 9: L'Assistant de création de volume de TrueCrypt affichant le panneau Emplacement du volume

Neuvième étape. **Cliquez** sur Suivant > pour afficher la *figure 10*.

2.3 Comment créer un volume standard sur une clé USB

Pour créer un volume **TrueCrypt** standard sur une clé USB, suivez les étapes 1 à 3 décrites à la section 2.2 Comment créer un volume standard afin d'activer la fenêtre *Type de volume*. Au lieu de choisir *Mes documents* comme emplacement, **naviguez** jusqu'à votre clé USB. **Nommez** ensuite votre fichier et **créez** votre *volume standard* à cet emplacement.

2.4 Comment créer un volume standard (suite)

À ce point, il faut déterminer une méthode de chiffrement spécifique (ou *algorithme* selon le vocabulaire du logiciel) pour encoder les données qui seront stockées dans le *volume standard*.

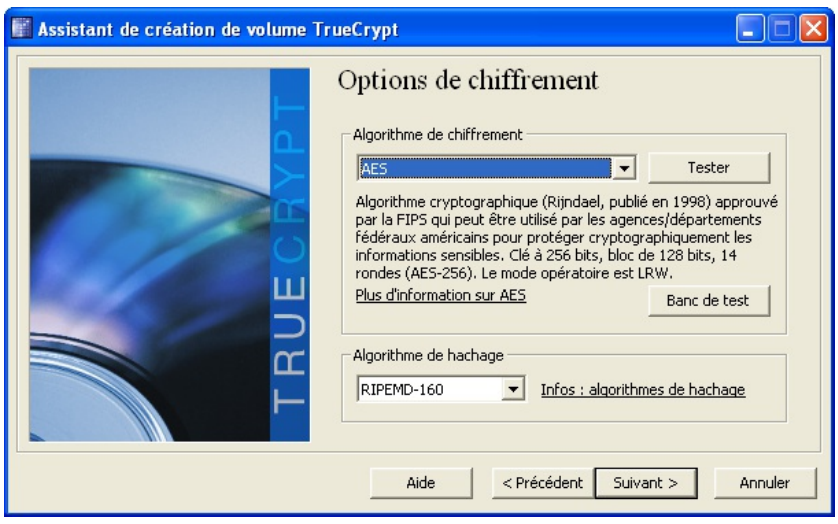

Assistant de création de volume TrueCrypt
TRUECRYPT
Options de chiffrement
Algorithme de chiffrement
AES
Tester
Algorithme cryptographique (Rijndael, publié en 1998) approuvé par la FIPS qui peut être utilisé par les agences/départements fédéraux américains pour protéger cryptographiquement les informations sensibles. Clé à 256 bits, bloc de 128 bits, 14 rondes (AES-256). Le mode opératoire est LRW.
Plus d'information sur AES
Banc de test
Algorithme de hachage
RIPEMD-160
Infos : algorithmes de hachage
Aide
< Précédent
Suivant >
Annuler

Figure 10: Le panneau Options de chiffrement

Commentaire: Vous pouvez laisser les options par défaut telles quelles. Tous les algorithmes présentés dans les deux options sont considérés sûrs.

Dixième étape. **Cliquez** sur [Suivant >] pour afficher la fenêtre *Taille du volume* de l'*Assistant de création de volume TrueCrypt*:

Assistant de création de volume TrueCrypt
Taille du volume
10
Ko
Mo
GB
Free space on drive C:\ is 27.42 GB
Please specify the size of the container you want to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.
Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.
TRUECRYPT
Aide
< Précédent
Suivant >
Annuler

Figure 11: La fenêtre Taille du volume

La fenêtre *Taille du volume* vous permet de préciser la taille du *volume standard*. Dans cet exemple, le volume est réglé à 10 Mo. Vous pouvez toutefois déterminer la taille qui vous convient. Prenez en considération les documents et les types de fichiers que vous voudrez stocker, ainsi que leur poids, et déterminez ensuite une taille de volume appropriée.

Astuce: Si vous avez l'intention de créer une copie de sauvegarde de votre *volume standard* sur un CD, vous devriez régler votre volume à 700 Mo.

Onzième étape. **Saisissez** la taille de volume souhaitée dans la zone de texte, puis **cliquez** sur [Suivant >] pour afficher la fenêtre suivante:

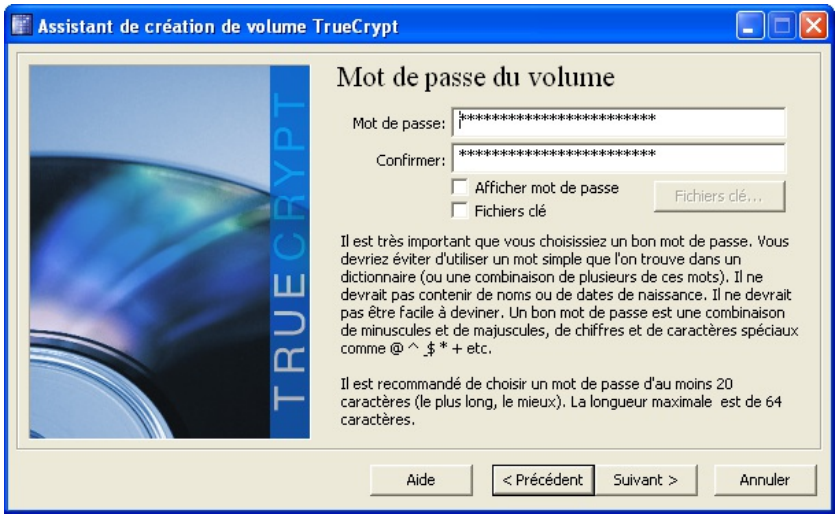

Assistant de création de volume TrueCrypt
Mot de passe du volume
Mot de passe:
Confirmer:
Afficher mot de passe
Fichiers clé
Fichiers clé...
Il est très important que vous choisissiez un bon mot de passe. Vous devriez éviter d'utiliser un mot simple que l'on trouve dans un dictionnaire (ou une combinaison de plusieurs de ces mots). Il ne devrait pas contenir de noms ou de dates de naissance. Il ne devrait pas être facile à deviner. Un bon mot de passe est une combinaison de minuscules et de majuscules, de chiffres et de caractères spéciaux comme @ ^ _$ * + etc.
Il est recommandé de choisir un mot de passe d'au moins 20 caractères (le plus long, le mieux). La longueur maximale est de 64 caractères.
TRUECRYPT
Aide
< Précédent
Suivant >
Annuler

*Figure 12: La fenêtre Mot de passe du volume *

Important: Le choix d'un mot de passe fort et sécuritaire est l'une des tâches les plus importantes à accomplir lors du processus de création d'un *volume standard*. Un bon mot de passe protégera efficacement un volume chiffré: plus votre mot de passe est fort, mieux votre volume sera protégé. Vous n'êtes pas obligé de créer vos propres mots de passe, ou même de vous en rappeler, si vous utilisez un programme de génération automatique de mots de passe comme **KeePass**. Veuillez consulter le Guide pratique **KeePass** [77] pour obtenir des renseignements sur la création et le stockage de mots de passe.

Douzième étape. **Saisissez** votre mot de passe, puis **saisissez-le** à nouveau dans les zones de texte *Mot de passe* et *Confirmer*.

Important: Le bouton *Suivant* demeurera désactivé tant et aussi longtemps que les mots de passe saisis dans les deux zones de texte ne correspondront pas. Si le mot de passe que vous avez choisi n'est pas particulièrement sûr, un message d'avertissement apparaîtra. Il est conseillé, dans ce cas, de changer de mot de passe! Cela dit, **TrueCrypt** fonctionnera tout de même avec le mot de passe que vous avez choisi, même si vos données ne seront pas particulièrement bien sécurisée.

Treizième étape. **Cliquez** sur [Suivant >] pour afficher la fenêtre suivante:

Figure 13: La fenêtre Formatage du volume

TrueCrypt est maintenant prêt à créer un volume standard. Bougez votre souris aléatoirement au dessus de la fenêtre de l'*Assistant de création de volume TrueCrypt* pendant au moins 30 secondes. Plus vous bougez votre souris longtemps, meilleure sera la qualité de la clé de chiffrement.

Quatorzième étape. **Cliquez** sur pour poursuivre la création de votre *volume standard*.

TrueCrypt créera un fichier nommé *Mon volume* dans le répertoire *Mes documents*, tel que spécifié plus tôt. Ce fichier contiendra un *volume TrueCrypt standard*, d'une taille de 10 Mo, que vous pourrez utiliser pour stocker vos fichiers de façon sécurisée.

Quand la création du *volume standard* sera achevée, cette boîte de dialogue apparaîtra : :

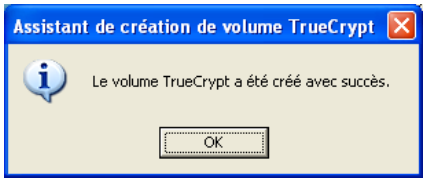
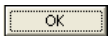


Figure 14: La boîte de dialogue Le volume TrueCrypt a été créé avec succès

Quinzième étape. **Cliquez** sur  pour finaliser la création du *volume standard* et revenir à la console **TrueCrypt**.

Seizième étape. **Cliquez** sur pour fermer l'*Assistant de création de volume TrueCrypt*.

Comment monter un volume standard

Sommaire des sections de cette page:

- **3.0 Comment monter un volume standard**
- **3.1 Comment démonter un volume standard**

3.0 Comment monter un volume standard

Dans **TrueCrypt**, *monter un volume* désigne le processus par lequel le volume est rendu accessible et prêt à l'utilisation. Dans cette section, vous apprendrez à *monter* le *volume standard* que vous venez de créer.

Pour entamer le montage du volume standard, suivez les étapes énumérées ci-dessous :

Première étape. **Double-cliquez** sur ou **Sélectionnez Démarrer > Programmes > TrueCrypt > TrueCrypt** pour ouvrir **TrueCrypt**.

Deuxième étape. **Sélectionnez** un lecteur dans la liste, comme suit :

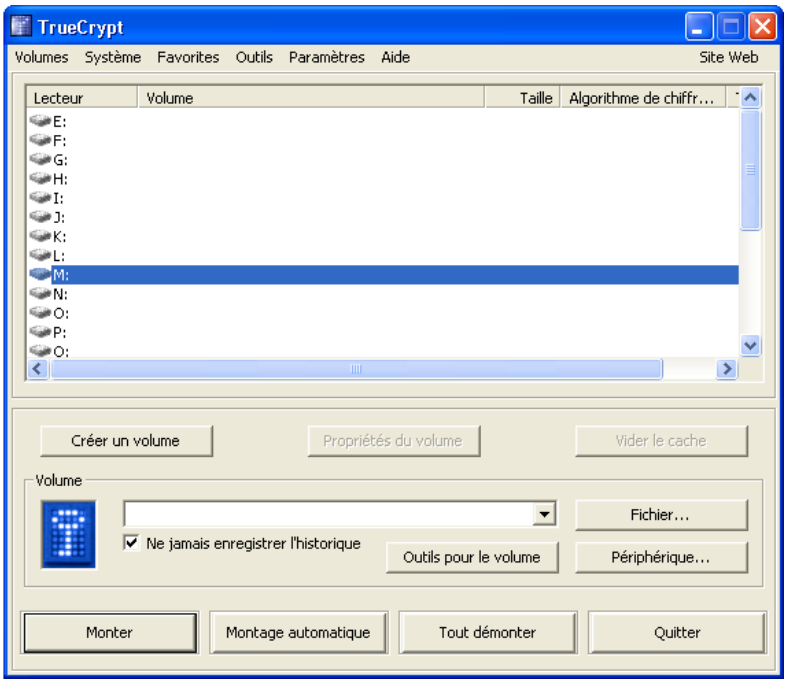


Figure 1: La console TrueCrypt

Dans cet exemple, le volume standard sera monté sur le lecteur M.

Commentaire: Dans la *figure 1*, le lecteur 'M' est sélectionné pour le montage du *volume standard*, mais vous pouvez choisir n'importe quel lecteur.

Troisième étape. **Cliquez** sur

La fenêtre Sélectionner un volume TrueCrypt apparaîtra:

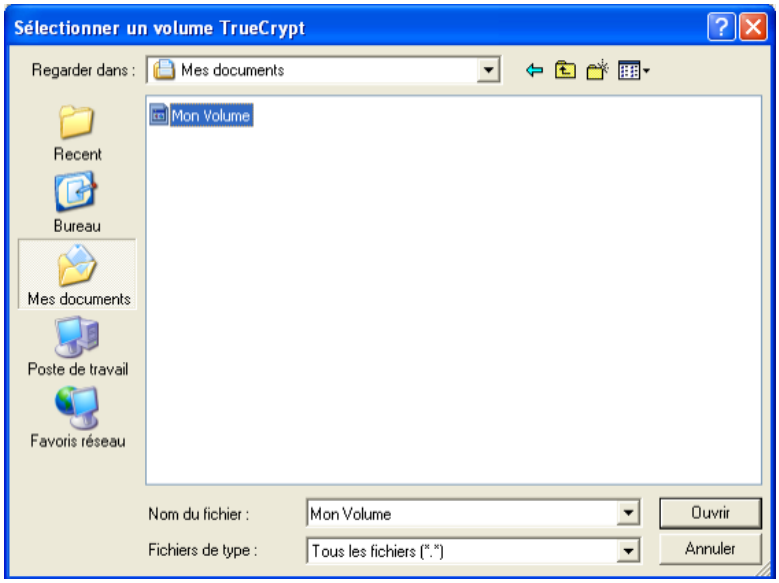


Figure 2: La fenêtre Sélectionner un volume TrueCrypt

Quatrième étape. **Sélectionnez** le fichier du *volume standard* que vous avez créé, puis **cliquez** sur

pour fermer la *figure 2* et revenir à la console **TrueCrypt**.

Cinquième étape. **Cliquez** sur

pour activer la fenêtre *Entrez le mot de passe pour...*, illustrée ci-dessous:

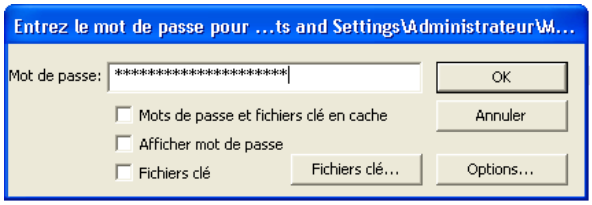


Figure 3: La fenêtre Entrez le mot de passe pour...

Sixième étape. **Saisissez** le mot de passe dans la zone de texte *Mot de passe:*.

Septième étape. **Cliquez** sur OK pour monter le *volume standard*.

Commentaire: Si le mot de passe que vous avez saisi est incorrect, **TrueCrypt** vous en avisera et vous devrez saisir le mot de passe de nouveau, puis **cliquer** sur OK. i cette fois-ci le mot de passe est correct, le volume standard sera monté:

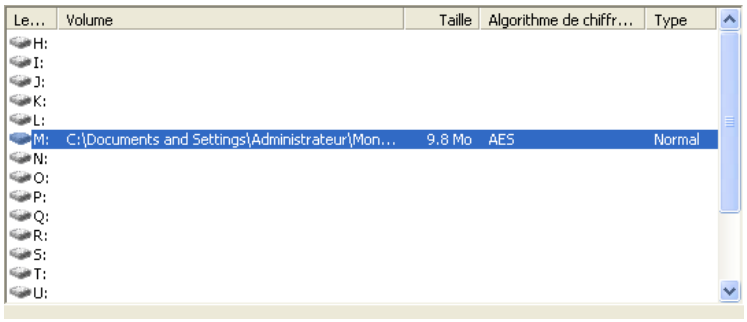


Figure 4: La console TrueCrypt affichant le volume standard nouvellement monté

Huitième étape. **Double-cliquez** sélection surlignée dans la liste **TrueCrypt** ou **double-cliquez** la lettre du disque correspondant dans la fenêtre *Poste de travail* pour accéder directement au *volume standard* maintenant monté sur le lecteur 'M:'.

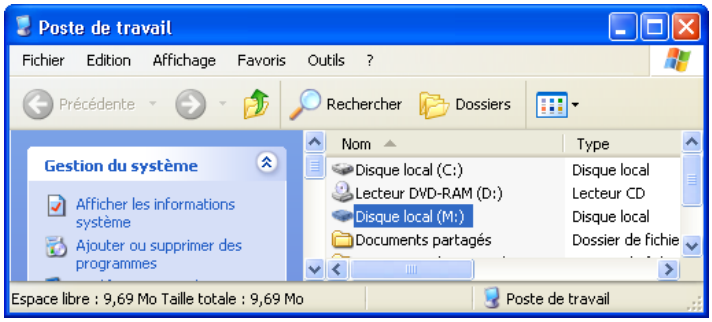


Figure 5: Accéder au volume standard via la fenêtre Poste de travail

Commentaire: Nous venons de monter le volume standard *Mon volume* en tant que lecteur virtuel *M:*. Ce lecteur virtuel a tous les attributs d'un vrai lecteur, sauf qu'il est complètement chiffré. Tous les fichiers copiés, déplacés ou sauvegardés dans ce disque virtuel seront automatiquement chiffrés (un processus appelé chiffrage à la volée).

Vous pouvez copier des fichiers dans le *volume standard*, exactement de la même façon qu'avec un lecteur normal (par exemple en le glissant depuis un autre répertoire). Lorsque vous déplacez un fichier depuis le *volume standard* vers un autre emplacement, celui-ci est automatiquement déchiffré. De la même façon, lorsque vous déplacez un fichier vers le *volume standard*, celui-ci est automatiquement chiffré. Lorsque votre ordinateur plante, ou s'il est soudainement éteint, **TrueCrypt** ferme automatiquement le *volume standard*.

Important: Après avoir transférer des fichiers dans le volume **TrueCrypt**, assurez-vous de ne laisser aucune trace de ces fichiers ailleurs sur l'ordinateur ou la clé USB dont ils proviennent. Veuillez consulter le chapitre **6. Détruire définitivement des données sensibles** [37] du livret pratique.

3.1 Comment démonter un volume standard

Dans **TrueCrypt*, le terme *démonter* désigne simplement le processus par lequel le volume est rendu inaccessible.

Pour fermer, ou démonter, un *volume standard* et faire en sorte que les fichiers qui s'y trouvent ne soient accessibles qu'aux personnes disposant du bon mot de passe, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez** le volume voulu dans la liste des volumes montés de la fenêtre principale de **TrueCrypt**:

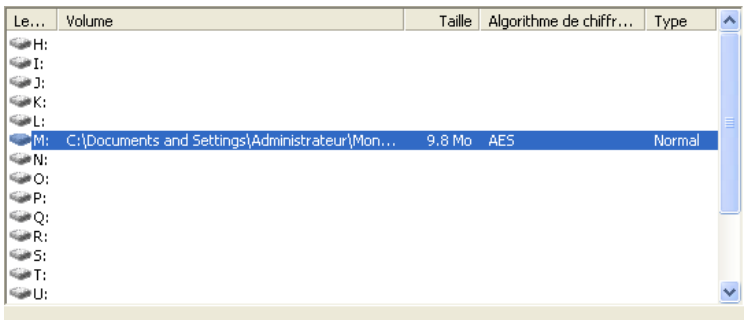


Figure 17: Sélectionner le volume standard à démonter

Deuxième étape. **Cliquez** sur Démonter pour démonter, ou fermer, le *volume standard* **TrueCrypt**.

Important: Assurez-vous de démonter votre volume **TrueCrypt** avant de mettre l'ordinateur en *veille* ou en *veille prolongée*. En

fait, il est plutôt conseillé d'éteindre le système complètement si vous avez l'intention de vous en éloigner. Cela empêchera tout intrus éventuel d'accéder au mot de passe de votre volume.

Pour récupérer les fichiers stockés dans votre volume standard, vous devrez monter le volume de nouveau.

Comment créer des copies de sauvegarde de vos volumes

Il est très important de créer régulièrement des copies de sauvegarde de vos documents, fichiers et répertoires. La copie de sauvegarde de votre *volume TrueCrypt standard* est essentielle et (heureusement) facile à réaliser. N'oubliez pas de démonter votre volume avant d'en faire une copie de sauvegarde.

Première étape. **Naviguez** jusqu'au fichier qui contient votre *volume standard* (dans la *figure 1*, ci-dessous, ce fichier se trouve dans le répertoire *Mes Documents*).

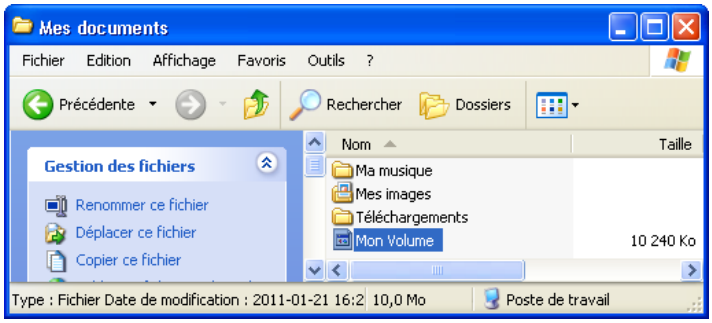


Figure 1: La recherche du fichier Mon Volume, dans la fenêtre Mes documents

Deuxième étape. **Sauvegardez** le fichier sur un support ou un dispositif de stockage amovible, comme un CD, un DVD ou une clé USB.

Astuce: Si vous avez une grande quantité de données que vous souhaitez chiffrer et archiver régulièrement, pourquoi ne pas créer un nouveau *volume standard* de la taille d'un CD ou d'un DVD? Cela peut être une technique d'archivage pratique et sécuritaire.

Avant de sauvegarder votre *volume standard* sur un support ou un dispositif amovible, assurez-vous que sa capacité de stockage correspond à la taille du volume.

Support de sauvegarde	Taille de volume TrueCrypt suggérée
CD	700 mo
DVD	3 900 mo
Clé USB	25% de la capacité de stockage totale (par ex. pour une clé USB de 128 Mo, utilisez 30 Mo pour votre volume standard)

Volumes cachés

Sommaire des sections de cette page:

- **5.0 À propos des volumes cachés**
- **5.1 Comment créer un volume caché**
- **5.2 Comment monter un volume caché**
- **5.3 Conseils sur l'utilisation sécuritaire de la fonction disque caché**

5.0 À propos des volumes cachés

Dans **TrueCrypt**, un *volume caché* est placé à l'intérieur de votre *volume standard* chiffré, mais son existence est dissimulée. Même si vous *montez* votre volume standard, il est impossible de trouver un volume caché, ou même d'en prouver l'existence. Dans l'éventualité où l'on vous forcerait à révéler votre mot de passe et l'emplacement de votre volume standard, le contenu de ce dernier serait révélé, mais l'existence du volume caché resterait occultée.

Imaginez une valise pourvue d'un double fond. Les dossiers de peu d'importance, dont la perte ou la confiscation ne vous dérange pas, sont conservés dans le compartiment normal, mais les dossiers importants et privés sont dissimulés dans le double fond. L'intérêt d'un compartiment secret (surtout s'il est bien conçu) est justement le secret: toute personne hostile ou malveillante n'en perçoit tout simplement pas l'existence. **TrueCrypt** utilise cette technique à votre avantage.

5.1 Comment créer un volume caché

La création d'un *volume caché* est semblable à celle d'un *volume standard*. Certains panneaux et fenêtres ont exactement la même apparence.

Première étape. **Ouvrez TrueCrypt**.

Deuxième étape. **Cliquez** sur Créer un volume pour afficher l'*Assistant de création de volume de TrueCrypt*.

Troisième étape. **Cliquez** sur Suivant > pour accepter l'option par défaut *Create an encrypted file container*.

Quatrième étape. **Cochez** l'option *Volume TrueCrypt caché*, comme suit:

Assistant de création de volume TrueCrypt
Type de volume
Volume TrueCrypt standard
Sélectionnez cette option si vous voulez créer un volume TrueCrypt normal.
Volume TrueCrypt caché
Il se peut que vous soyez forcé par quelqu'un de révéler votre mot de passe. Il y a des situations où vous ne pouvez pas refuser de divulguer le mot de passe (ex: par une extorsion). L'utilisation d'un volume caché vous permet de résoudre de telles situations sans donner le mot de passe de votre volume.
Plus d'infos sur les volumes cachés
Aide
< Précédent
Suivant >
Annuler
TRUECRYPT

Figure 1: L'Assistant de création de volume TruCrypt avec l'option Volume TrueCrypt caché sélectionné

Cinquième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

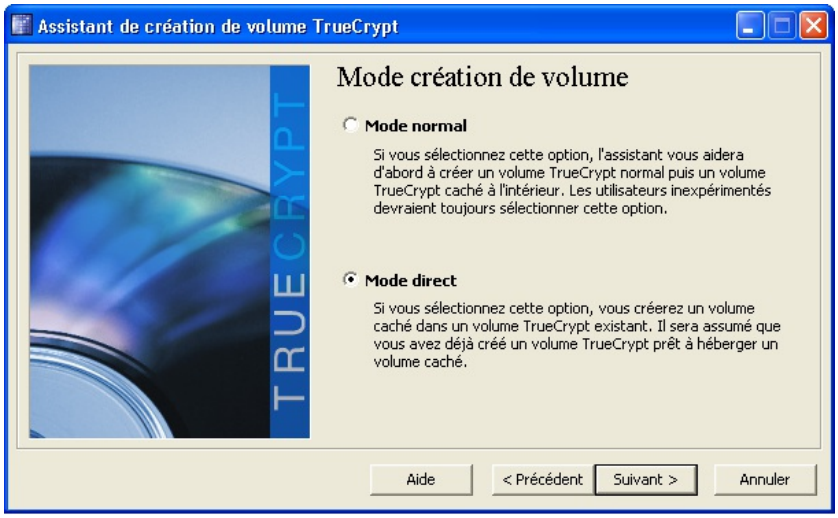

Assistant de création de volume TrueCrypt
Mode création de volume
Mode normal
Si vous sélectionnez cette option, l'assistant vous aidera d'abord à créer un volume TrueCrypt normal puis un volume TrueCrypt caché à l'intérieur. Les utilisateurs inexpérimentés devraient toujours sélectionner cette option.
Mode direct
Si vous sélectionnez cette option, vous créerez un volume caché dans un volume TrueCrypt existant. Il sera assumé que vous avez déjà créé un volume TrueCrypt prêt à héberger un volume caché.
Aide
< Précédent
Suivant >
Annuler
TRUECRYPT

Figure 2: La fenêtre Mode création de volume

- *Mode direct*: Cette option vous permet de créer un volume caché dans un *volume standard* existant.
- *Mode normal*: Cette option vous permet de créer un nouveau *volume standard*, à l'intérieur duquel vous incorporerez un *volume caché*.

Pour les fins de cet exercice, **cochez** l'option *Mode direct*.

Commentaire: Si vous souhaitez plutôt créer un nouveau *volume standard*, répétez les étapes détaillées à la section **2.2 Comment créer un volume standard** [78].

Sixième étape. **Cochez** l'option *Mode direct*, puis **cliquez** sur Suivant > pour afficher la fenêtre *Sélectionner un volume TrueCrypt*.

Commentaire: Assurez-vous que le *volume standard* est démonté lorsque vous le sélectionnez.

Septième étape. **Cliquez** sur Fichier... pour afficher la fenêtre suivante:

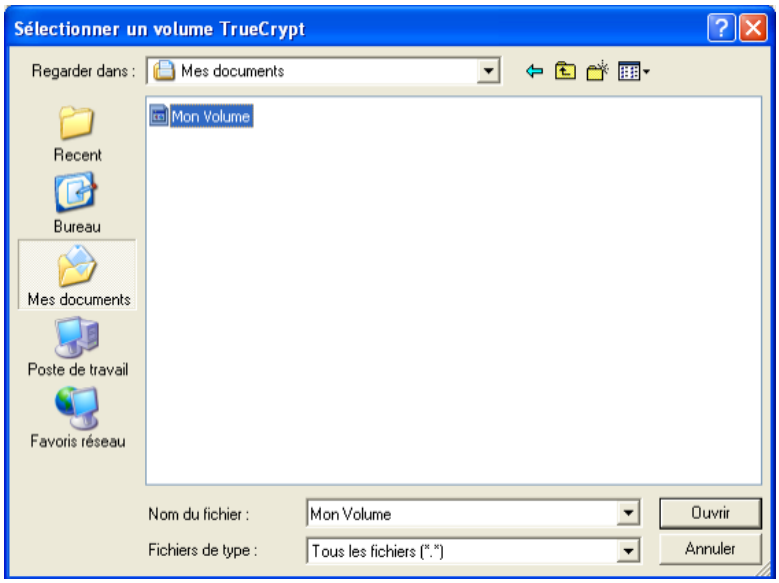


Figure 3: La fenêtre Sélectionner un volume TrueCrypt

Huitième étape. **Trouvez** le fichier du volume à l'aide de la fenêtre *Sélectionner un volume TrueCrypt*, tel qu'illustré à *figure 3*.

Neuvième étape. **Cliquez** sur Ouvrir pour revenir à l'*Assistant de création de volume*.

Dixième étape. **Cliquez** sur OK pour afficher la fenêtre *Mot de passe du volume*.

Onzième étape. **Saisissez** le mot de passe que vous avez utiliser lors de la création du *volume standard* dans la zone de texte *Mot de passe* pour afficher la fenêtre suivante:

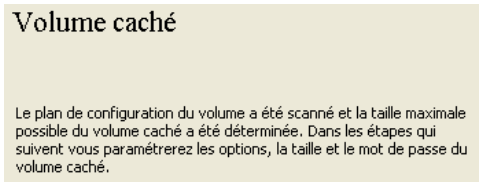

Volume caché
Le plan de configuration du volume a été scanné et la taille maximale possible du volume caché a été déterminée. Dans les étapes qui suivent vous paramétrerez les options, la taille et le mot de passe du volume caché.

Figure 4: Le panneau volume caché

Douzième étape. **Cliquez** sur Suivant > après avoir lu le message pour afficher la fenêtre *Options de chiffrement du volume caché*.

Commentaire: Laissez les options de l'*Algorithme de chiffrement* et l'*Algorithme de hachage* du *volume caché * telles quelles.

Treizième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

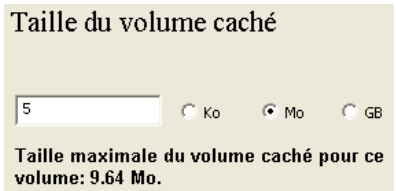


Figure 5: La fenêtre Taille du volume caché

Il faut maintenant choisir la taille du *volume caché*.

Commentaire: Tenez compte du type de documents, de leur taille ainsi que de la quantité de fichiers à stocker. N'oubliez pas de laisser de l'espace pour le *volume TrueCrypt standard*. Si vous choisissez la taille maximale disponible pour votre *volume caché*, vous ne pourrez plus stocker de fichiers dans le *volume standard* original.

Si votre *volume standard* est de 10 Mo et que vous indiquez que votre volume caché doit avoir 5 Mo (tel qu'illustré à la *figure 5*, ci-dessus), vous aurez deux volumes (un standard et l'autre caché) d'approximativement 5 Mo chacun.

Dans ce cas, vous devez vous assurer que les données que vous stockerez dans le *volume standard* ne dépassent pas 5 Mo. Le programme **TrueCrypt** ne détecte pas automatiquement l'existence d'un *volume caché* (par mesure de sécurité) et il est donc possible que les données qui s'y trouvent soient écrasées par mégarde. Vous risquez de perdre les données contenues dans le volume caché si vous dépassez la taille que vous aviez fixée.

Quatorzième étape. **Saisissez** la taille que vous souhaitez pour votre *volume caché* dans la zone appropriée de la fenêtre illustrée à la *figure 5*.

Quinzième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Mot de passe du volume caché*.

Vous devez maintenant choisir pour votre *volume caché* un mot de passe *différent* de celui que vous avez attribué au *volume*

standard. N'oubliez pas de choisir un mot de passe fort. Pour plus d'information sur la création de mot de passes forts, voir le Guide pratique **KeePass** [77]. Vous devez absolument choisir un mot de passe différent de celui utilisé pour le volume standard.

Astuce: Si vous craignez qu'advienne une situation où vous êtes forcé de révéler le contenu de vos *volumes TrueCrypt*, archivez le mot de passe du *volume standard* dans **KeePass**, puis créez un mot de passe fort que vous mémoriserez pour le *volume caché*. Cela contribuera à protéger davantage le *volume caché*, puisque vous ne laisserez aucune trace de son existence.

Seizième étape. **Créez** un mot de passe, **saisissez-le** deux fois, puis **cliquez** sur Suivant > pour afficher la fenêtre suivante:

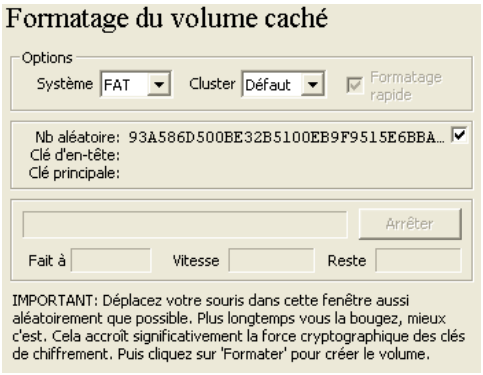

Formatage du volume caché
Options
Système FAT
Cluster Défaut
Formatage rapide
Nb aléatoire: 93A586D500BE32B5100EB9F9515E6BBA...
Clé d'en-tête:
Clé principale:
Arrêter
Fait à
Vitesse
Reste
IMPORTANT: Déplacez votre souris dans cette fenêtre aussi aléatoirement que possible. Plus longtemps vous la bougez, mieux c'est. Cela accroît significativement la force cryptographique des clés de chiffrement. Puis cliquez sur 'Formater' pour créer le volume.

Figure 6: La fenêtre Formatage du volume caché

Laissez les options *Système* et *Cluster* telles qu'elles.

Dix-septième étape. **Bougez** la souris au dessus de la fenêtre pour accroître la force de chiffrement, puis **cliquez** sur Formater pour formater le *volume caché*.

Lorsque le formatage du volume caché est complété, vous verrez apparaître une fenêtre semblable à celle-ci:

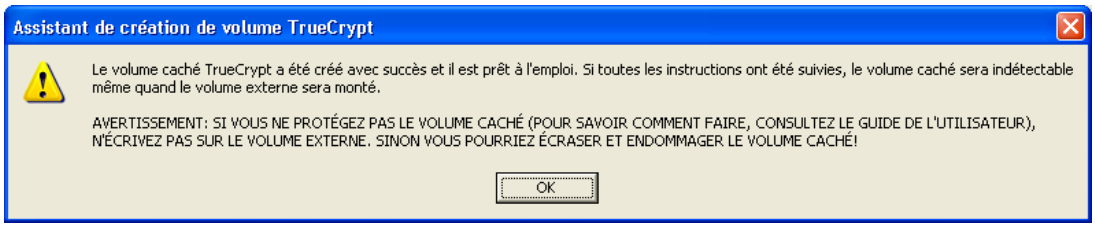

Assistant de création de volume TrueCrypt
Le volume caché TrueCrypt a été créé avec succès et il est prêt à l'emploi. Si toutes les instructions ont été suivies, le volume caché sera indétectable même quand le volume externe sera monté.
AVERTISSEMENT: SI VOUS NE PROTÉGEZ PAS LE VOLUME CACHÉ (POUR SAVOIR COMMENT FAIRE, CONSULTEZ LE GUIDE DE L'UTILISATEUR), N'ÉCRIVEZ PAS SUR LE VOLUME EXTERNE. SINON VOUS POURRIEZ ÉCRASER ET ENDOMMAGER LE VOLUME CACHÉ!
OK

Figure 7: Fenêtre d'avertissement de l'Assistant de création de volume

Commentaire: La *Figure 7* ci-dessus confirme que vous avez bien créé un *volume caché* et vous rappelle le risque d'écraser des fichiers dans le *volume caché* lorsque vous stockez des fichiers dans le *volume standard* original.

Dix-huitième étape. **Cliquez** sur OK pour afficher la fenêtre *Volume caché créé*, puis **cliquez** sur Quitter pour revenir à la console **TrueCrypt**.

Le *volume caché* a été créé à l'intérieur de votre *volume standard*. Cela vous permet de cacher des documents à l'intérieur de votre *volume standard*. Ceux-ci resteront invisibles, même pour une personne qui a réussi à obtenir le mot de passe de ce *volume standard*.

5.2 Comment monter un volume caché

La méthode pour accéder à un *volume caché* est exactement de la même que pour un *volume standard*. La seule différence est que vous devez utiliser le mot de passe du *volume caché* plutôt que celui du *volume standard*. C'est par le mot de passe que **TrueCrypt** détermine s'il doit ouvrir le *volume standard* ou le *volume caché*.

Pour *monter*, ou ouvrir, le volume caché, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez** un lecteur dans la liste (dans cet exemple, le lecteur *K*):

Figure 8: Un lecteur sélectionné dans la fenêtre des volumes de TrueCrypt

Deuxième étape. **Cliquez** sur Fichier... pour afficher la fenêtre *Sélectionnez un volume TrueCrypt*.

Troisième étape. **Naviguez** jusqu'à votre fichier de volume **TrueCrypt** (le même fichier que pour votre *volume standard*), puis **sélectionnez-le**.

Quatrième étape. **Cliquez** sur Ouvrir pour revenir à la console **TrueCrypt**.

Cinquième étape. **Cliquez** sur Monter pour afficher la fenêtre *Entrez le mot de passe pour...*, tel qu'illustré ci-dessous:

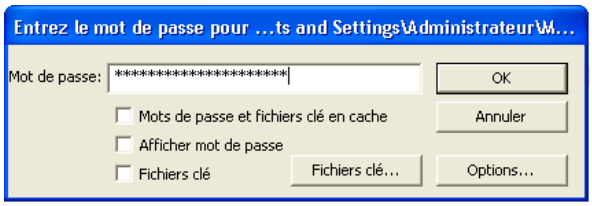


Figure 9: La fenêtre Entrez le mot de passe pour...

Sixième étape. **Saisissez** e mot de passe que vous avez choisi lors de la création du *volume caché*, puis **cliquez** sur OK.

Le *volume caché* est maintenant monté (ouvert), tel qu'illustré ci-dessous:

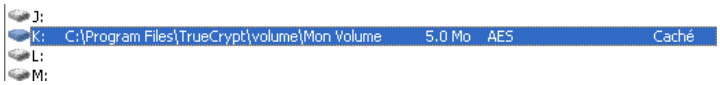


Figure 10: La fenêtre principale de TrueCrypt affichant le volume caché récemment monté

Septième étape. **Double-cliquez** sur cette entrée ou passer par la fenêtre *Poste de travail*.

5.3 Conseils sur l'utilisation sécuritaire de la fonction disque caché

Le but de la fonction lecteur caché est de vous soustraire à toute situation potentiellement dangereuse en *laissant l'impression* à un adversaire que vous lui donnez ce qu'il veut - l'accès à vos fichiers - sans pour autant compromettre la sécurité de vos données. En plus de protéger vos données, cela vous permet d'éviter de vous mettre davantage en danger ou d'exposer vos collègues et partenaires. Pour que cette technique soit efficace, vous devez créer une situation où votre adversaire sera satisfait des résultats de sa recherche et cessera de vous importuner.

Pour que cela soit efficace, vous devriez suivre ces quelques indications:

- Placez vos documents semi-sensibles, ceux dont la perte vous dérange moins, dans le *volume standard*. Ces documents doivent tout de même être assez "intéressants" pour capter l'attention de votre adversaire lorsque vous serez forcé de les lui montrer.
- Gardez à l'esprit que votre adversaire est peut être conscient de la possibilité de créer des *volumes cachés* avec **TrueCrypt**. Cela dit, si vous utilisez **TrueCrypt** correctement, cette personne ne sera pas en mesure de prouver l'existence d'un volume caché, ce qui rendra votre démenti plus crédible.
- Actualisez régulièrement (une fois par semaine) les fichiers placés dans le *volume standard*. Cela donnera l'impression que vous utilisez réellement ces fichiers.

Lorsque vous montez un volume **TrueCrypt**, il vous est toujours possible d'activer la fonction *Empêcher les dommages causés en écrivant dans le volume externe*. C'est une option extrêmement importante qui vous permet d'ajouter des fichiers de "diversion" à votre *volume standard* sans devoir vous inquiéter de supprimer ou d'écraser le contenu chiffré de votre *volume caché*.

Comme nous l'avons déjà vu, il existe un risque que vous écrasiez vos fichiers cachés lorsque vous dépassez la limite d'espace que vous avez déterminée pour votre *volume standard*. Vous ne devriez jamais activer l'option *Protection du volume caché* lorsque vous êtes forcé par quelqu'un de monter un volume **TrueCrypt**, parce que vous seriez alors obligé de saisir le mot de passe secret de votre *volume caché* et cela révélerait automatiquement l'existence dudit volume. Lorsque vous actualisez vos fichiers de "diversion" en privé, par contre, vous devriez *toujours* activer cette option.

Pour utiliser l'option *Protection du volume caché*, suivez les étapes énumérées ci-dessous.

Première étape. **Cliquez** sur Options... de la fenêtre *Entrez le mot de passe pour...* illustrée à la *figure 9*, ci-dessus, pour afficher la fenêtre *Options de montage*, illustrée ci-dessous:

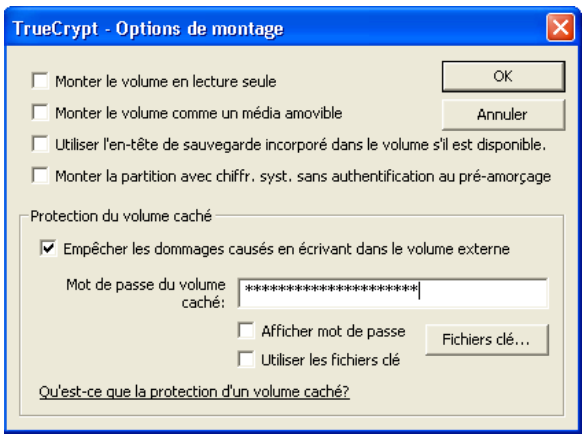

TrueCrypt - Options de montage
Monter le volume en lecture seule
Monter le volume comme un média amovible
Utiliser l'en-tête de sauvegarde incorporé dans le volume s'il est disponible.
Monter la partition avec chiffr. syst. sans authentification au pré-amorçage
OK
Annuler
Protection du volume caché
Empêcher les dommages causés en écrivant dans le volume externe
Mot de passe du volume caché:
Afficher mot de passe
Utiliser les fichiers clé
Fichiers clé...
Qu'est-ce que la protection d'un volume caché?

Figure 11: La fenêtre Options de montage

Deuxième étape. **Cochez** l'option *Empêcher les dommages causés en écrivant dans le volume externe*.

Troisième étape. **Saisissez** le mot de passe de votre *volume caché*, puis **cliquez** sur

.

Quatrième étape. **Cliquez** sur

pour monter votre *volume standard*. Lorsque celui-ci sera monté, vous serez en mesure d'ajouter des fichiers de "diversion" sans endommager les fichiers stockés dans votre *volume caché*.

Cinquième étape. **Cliquez** sur

pour démonter votre *volume standard* quand vous avez fini d'en actualiser le contenu.

N'oubliez pas: Vous ne devez effectuer cette opération que lorsque vous actualisez les fichiers qui se trouvent dans votre *volume standard*. Lorsque vous révélez l'existence de votre volume standard à quelqu'un, vous ne devriez pas utiliser la fonction *Protection du volume caché*.

Faq et questions récapitulatives

6.0 Faq et questions récapitulatives

Claudia et Pablo sont satisfaits de ce que leur offre **TrueCrypt**, d'autant plus que le programme est facile à installer et fonctionne maintenant automatiquement. Cependant, avant de décider définitivement de l'utiliser, ils ont encore quelques questions à propos de **TrueCrypt**.

Q: *Est-ce que je vais devoir passer tout mon temps à saisir des mots de passe?*

A: *Non, tu n'auras qu'à saisir ton mot de passe une seule fois, à l'ouverture du volume standard. Lorsque cela est fait, tu peux ouvrir tous les fichiers contenu dans le volume sans devoir saisir de mots de passe.*

Q: *Puis-je désinstaller **TrueCrypt** facilement si je n'en veux plus? Si je désinstalle le programme, mes fichiers seront-ils toujours chiffrés?*

A: *Oui, on peut facilement désinstaller **TrueCrypt** en **sélectionnant Démarrer > Programmes > Truecrypt > Uninstall Truecrypt**.*

*Cependant, tu dois retirer tous tes fichiers du volume standard avant de désinstaller le programme, sinon il ne te sera plus possible d'y accéder, à moins de réinstaller **TrueCrypt** ou de transférer le fichier du volume standard sur un ordinateur où est installé le programme. Si tu transfères ton volume standard sur un autre ordinateur, tu auras toujours besoin du bon mot de passe pour y accéder.*

Q: *Si j'ai un problème avec **TrueCrypt**, y a t-il une adresse de courriel ou un site Internet où je peux trouver de l'aide?*

A: *Pour obtenir du soutien technique, consulte la documentation en ligne sur le site de **TrueCrypt** **http://www.TrueCrypt.org/docs/** [75] ou sur le forum à **http://forums.truecrypt.org//** [79], ou encore sur le site Internet Security Box **http://security.ngoinabox.org/fr/truecrypt_principale** [80]. Cela dit, personne ne pourra retrouver un mot de passe oublié!*

Q: *Est-ce que différentes versions de **Windows** affichent différents formats de fenêtre lorsqu'on utilise **TrueCrypt**?*

A: *L'apparence des fenêtres peut varier un peu, mais le contenu est toujours le même.*

Q: *Quels types de fichiers doit-on chiffrer?*

A: *Idéalement, tu devrais chiffrer tous tes documents, images ou fichiers qui contiennent des renseignements privés ou sensibles. S'il advenait que ton ordinateur soit perdu ou confisqué, l'information comprise dans ton volume **TrueCrypt** serait à l'abri.*

Q: *Dans quelle mesure nos fichiers seront-ils sécurisés?*

A: ***TrueCrypt** a été testé de façon indépendante par des spécialistes de la sécurité informatique pour évaluer sa performance et déterminer si toutes les fonctions incluses dans le programme opèrent tel qu'annoncé. Les résultats de ces examens révèlent que **TrueCrypt** est un excellent programme, qui offre un niveau élevé de protection. Le choix d'un mot de passe fort est essentiel pour préserver la sécurité de vos volumes.*

La fonction de volume caché de *TrueCrypt* présente un niveau de sécurité exceptionnel pour les données stockée sur votre ordinateur. L'utilisateur doit avoir une excellente maîtrise du programme et de ses fonctions de base, ainsi qu'une bonne compréhension de ses propres risques en terme de sécurité et des situations où la fonction de volume caché peut s'avérer utile.

Q: *Est-il possible d'endommager ou détruire le disque caché par inadvertance?*

A: *Oui. Si vous continuez d'ajouter des fichiers au volume standard jusqu'à ce qu'il n'y ait plus assez d'espace (pour que le volume caché puisse exister), votre volume caché sera automatiquement écrasé. Il existe une option dans le menu de **TrueCrypt** qui sert à protéger votre volume caché contre l'écrasement ou la suppression accidentelle, mais l'utilisation de cette fonctionnalité peut révéler l'existence d'un volume caché.*

Q: *Puis-je modifier la taille de mon volume caché après l'avoir créé?*

A: *Non. Il vous faudra créer un autre volume caché et y transférer vos fichiers manuellement*

Q: *Puis-je utiliser 'chkdsk', 'Défragmenteur de disque', ou d'autres outils semblables sur un volume monté **TrueCrypt**?*

A: *Les volumes **TrueCrypt** se comportent exactement comme de vrais disques. Il est donc possible d'utiliser n'importe quel outil de vérification, de réparation ou de défragmentation du contenu sur un volume **TrueCrypt**.*

Q: *Est-il possible de changer le mot de passe d'un volume caché?*

A: *Oui. La fonction 'Modifier le mot de passe du volume' s'applique aussi bien aux volumes cachés qu'aux volumes standards. Vous n'avez qu'à saisir le mot de passe actuel du volume caché dans la zone de texte Mot de passe actuel de la fenêtre de l'option 'Modifier le mot de passe du volume'.*

Q: *Quand devrais-je utiliser la fonction de volume caché?*

A: *Utilisez la fonction de volume caché de* ***TrueCrypt*** *lorsque vous devez dissimuler l'existence de certains renseignements se trouvant sur votre ordinateur. Notez bien que cela est différent de l'utilisation d'un volume standard, qui sert essentiellement à protéger l'accès à vos renseignements.*

Pour une foire aux questions détaillée à propos de **TrueCrypt**, **http://www.TrueCrypt.org/faq.php** [81]

6.1 Questions récapitulatives portant sur les volumes standards

- Qu'est-ce que le chiffrement?
- Qu'est-ce qu'un *volume standard*?
- Comment peut-on créer un *volume standard* sur une clé USB?
- Quels sont les différentes façon de démonter un *volume standard*?
- Comment peut-on choisir et conserver un bon mot de passe pour protéger un *volume standard*?
- Quelles sont les options pour la création d'une copie de sauvegarde de votre *volume standard*?
- Décrivez quelques une des méthodes utilisées pour dissimuler la présence du *volume standard* sur votre ordinateur.

6.2 Questions récapitulatives portant sur les volumes cachés

- Quel est la principale différence entre un *volume standard* et un *volume caché*?
- Quel types de fichiers devraient être placés dans un *volume standard* si vous utilisez aussi un *volume caché*?
- Où est situé le *volume caché*?
- Quel est la taille idéale d'un *volume caché*?
- Quels sont les avantages et désavantages associés à l'option qui protège votre *volume caché* contre une suppression ou un écrasement accidentel?

Cobian - copies de sauvegarde

Cobian Backup sert à créer des copies de sauvegarde ou des « archives » de vos fichiers et répertoires. Les copies de sauvegarde peuvent être stockées dans d'autres répertoires ou lecteurs de votre ordinateur, sur les autres ordinateurs d'un réseau de travail ou sur des supports amovibles.

Site Internet

www.educ.umu.se/~cobian/cobianbackup.htm [82]

Configuration requise :

- Windows NT/2000/XP/Vista (version 8)
- Windows 95, 98, ME sont compatibles avec la version 7 [83] de Cobian Backup

Version utilisée pour rédiger ce guide :

- 8.4.0.202

Pour installer Cobian

- *Lisez la courte introduction des Guides pratiques [13]*
- ***Cliquez sur l'icône ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.*
- *Lisez attentivement la 'Notice d'installation' avant de continuer.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

Cobian:

[84]

Licence :

- Gratuiciel (*Freeware*)

Lecture préalable :

- Livret pratique Security in-a-box, chapitre 5. Récupérer des données perdues [85].

Niveau : 1 : Débutant, 2 : Moyen, **3 : intermédiaire**, 4 : Expérimenté, 5 : Avancé

Temps d'apprentissage : 30 minutes

Ce que vous apportera l'utilisation de cet outil :

- La capacité de créer des copies de sauvegarde pour tous vos documents, fichiers et répertoires.
- La capacité de compresser et décompresser vos fichiers de sauvegarde.
- La capacité de chiffrer et déchiffrer vos fichiers archivés.

1.1 À propos de cet outil

Cobian Backup sert à créer des copies de sauvegarde ou des "archives" de vos fichiers et répertoires. Les copies de sauvegarde peuvent être stockées dans d'autres répertoires ou lecteurs de votre ordinateur, sur les autres ordinateurs d'un réseau de travail ou sur des supports amovibles (CD, DVD et clés USB). Vous pouvez planifier le moment où des copies de sauvegarde de fichiers et de répertoires devront être créées. Le programme peut rouler en arrière-plan de votre système (c'est-à-dire dans la barre des tâches de votre système), consulter votre horaire et générer des copies de sauvegarde lorsque cela est nécessaire. Cobian Backup peut également compresser et chiffrer des fichiers en même temps qu'il crée les copies de sauvegarde.

1.2 Commentaire sur l'installation

Durant le processus d'installation, vous devrez régler une série d'options. Nous recommandons de **cocher** l'option *en tant que service* pour vous assurer que le programme soit actif en tout temps (en arrière-plan) et que vos copies de sauvegarde soient créées automatiquement en temps voulu.

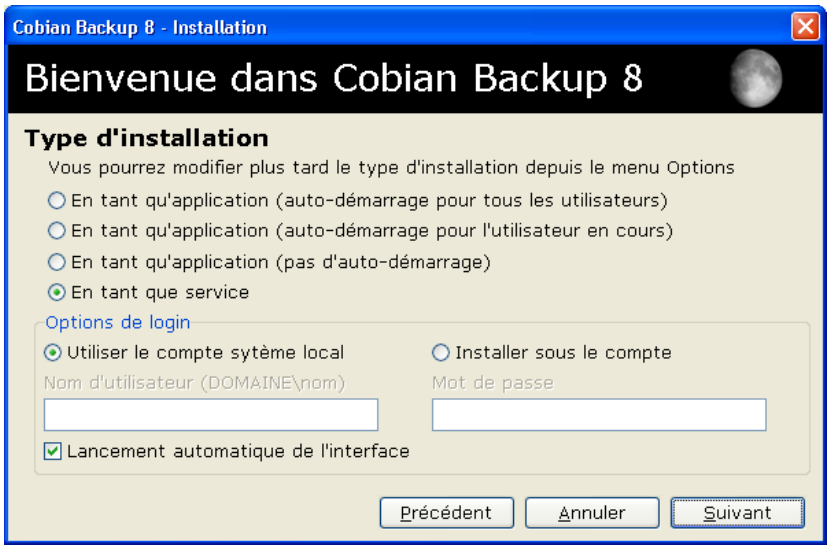

Cobian Backup 8 - Installation
Bienvenue dans Cobian Backup 8
Type d'installation
Vous pourrez modifier plus tard le type d'installation depuis le menu Options
En tant qu'application (auto-démarrage pour tous les utilisateurs)
En tant qu'application (auto-démarrage pour l'utilisateur en cours)
En tant qu'application (pas d'auto-démarrage)
En tant que service
Options de login
Utiliser le compte sytème local
Installer sous le compte
Nom d'utilisateur (DOMAINE\nom)
Mot de passe
Lancement automatique de l'interface
Précédent
Annuler
Suivant

Figure 1 : La fenêtre d'installation de Cobian Backup 8

Créer une copie de sauvegarde

Cette section aborde les configurations minimales nécessaires à la création de copies de sauvegarde de groupes de fichiers. D'autres sections aborderont la compression et/ou le chiffrage des copies de sauvegarde des fichiers. **Cobian Backup** vous permet de créer des tâches de sauvegarde qui peuvent être configurées pour inclure un groupe particulier de fichiers et/ou de répertoires. Vous pouvez régler le programme pour que ces tâches de sauvegarde soient exécutées à des heures et des jours déterminés.

Pour créer une tâche de sauvegarde, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur : pour créer une nouvelle tâche de sauvegarde.

Ceci active la fenêtre *Propriétés de:*

Le menu de gauche vous offre d'activer les différentes fenêtres et d'établir les paramètres nécessaires à la procédure de sauvegarde.

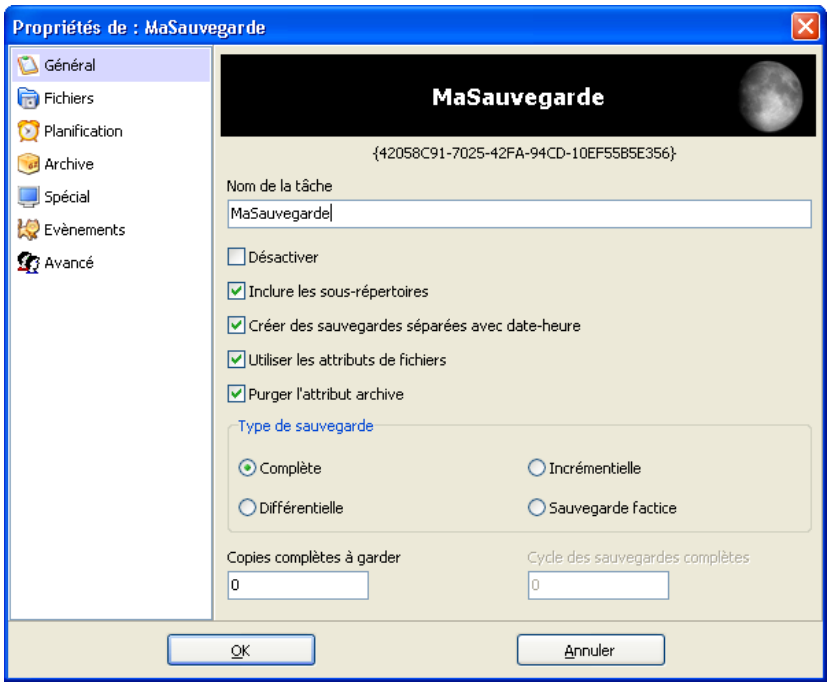


Figure 2 : La fenêtre Propriétés de: affichant le nom du fichier MaSauvegarde nouvellement créé

2.1 Description des options

Nom de la tâche : Sélectionnez un nom pour la tâche. Utilisez un nom qui désigne la nature de la copie de sauvegarde. Par exemple, si la copie de sauvegarde contiendra les fichiers vidéo, vous pouvez la nommer *Copie de sauvegarde vidéo*.

Désactiver : Laissez la case *désactiver* non cochée. **Avertissement** : Si vous cochez cette option, la tâche ne s'exécutera pas.

Inclure les sous-répertoires : Si cette option est cochée, tout dossier qui se trouve dans le dossier que vous avez sélectionné sera inclus. Cette méthode est efficace pour créer des copies de sauvegarde d'un grand nombre de fichiers. Par exemple : si vous sélectionnez le dossier *Mes documents* et cochez cette option, tous les fichiers et dossiers dans Mes documents seront inclus dans la copie de sauvegarde.

Créer des copies de sauvegarde séparées avec date-heure : Cette option signifie qu'une fois la copie de sauvegarde terminée, l'heure et la date à laquelle elle a été créée apparaîtra dans le nom du dossier qui contient la copie de sauvegarde. Cette option est intéressante parce qu'elle vous permettra de reconnaître facilement le moment où la copie de sauvegarde a été créée.

Utiliser les attributs de fichiers : Cette option n'est utile que si vous choisissez de créer une copie de sauvegarde incrémentielle ou différentielle (voir détails ci-dessous). Les attributs de fichiers contiennent de l'information au sujet du fichier.

Cobian Backup vérifie cette information afin de déterminer si un changement a été apporté au fichier source depuis la dernière fois qu'une copie de sauvegarde a été créée. Si vous exécutez une copie de sauvegarde incrémentielle ou différentielle, le fichier sera mis à jour. **Commentaire** : Vous ne serez en mesure d'exécuter une copie de sauvegarde complète ou "factice" que si vous décochez cette option (la copie de sauvegarde "factice" est expliquée ci-dessous).

2.2 Description des types de copies de sauvegarde

Complète : Tous les fichiers se trouvant à l'emplacement source seront copiés dans votre répertoire de copies de sauvegarde. Si vous cochez l'option *Créer des copies de sauvegarde séparées avec date-heure*, vous aurez plusieurs copies provenant de la même source (identifiées au moyen de l'heure et de la date, incluses dans le nom du fichier, où la copie a été créée). Autrement dit, le programme écrasera la version antérieure (s'il en existe une).

Incrémentielle : Le programme vérifiera si les fichiers source ont été modifiés depuis la création de la plus récente copie de sauvegarde. Le programme ignorera les fichiers qui n'ont pas besoin d'être copiés, ce qui économisera du temps. L'option *Utiliser les attributs de fichiers* doit être cochée pour que ce type de sauvegarde puisse être exécutée.

Bit d'archive : Il s'agit d'information sur la taille du fichier et sur la date de création et de modification. Cette information permet à Cobian Backup de déterminer si le fichier a été modifié par vous depuis la dernière création d'une copie de sauvegarde.

Différentielle : Le programme vérifiera si la source a été modifiée depuis la dernière création d'une copie de sauvegarde **complète**. Le programme ignorera les fichiers qui n'ont pas besoin d'être copiés, ce qui économisera du temps. Si vous avez auparavant exécuté une copie de sauvegarde complète du même groupe de fichiers, vous pouvez alors continuer à créer des copies de sauvegarde en utilisant la méthode différentielle.

Sauvegarde factice : Cette option correspond à une fonction de copie de sauvegarde dont nous n'avons pas vraiment besoin. Tu peux l'utiliser pour que ton ordinateur exécute ou ferme certains programmes à des moments précis. Cette option, de niveau avancé, est peu utile à nos procédures de copie de sauvegarde.

2.3 Comment créer un fichier de sauvegarde

Pour démarrer la création d'un fichier de sauvegarde, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur l'icône *Fichiers* dans le coin gauche de la fenêtre *Propriétés de:* pour sélectionner les fichiers qui seront copiés.

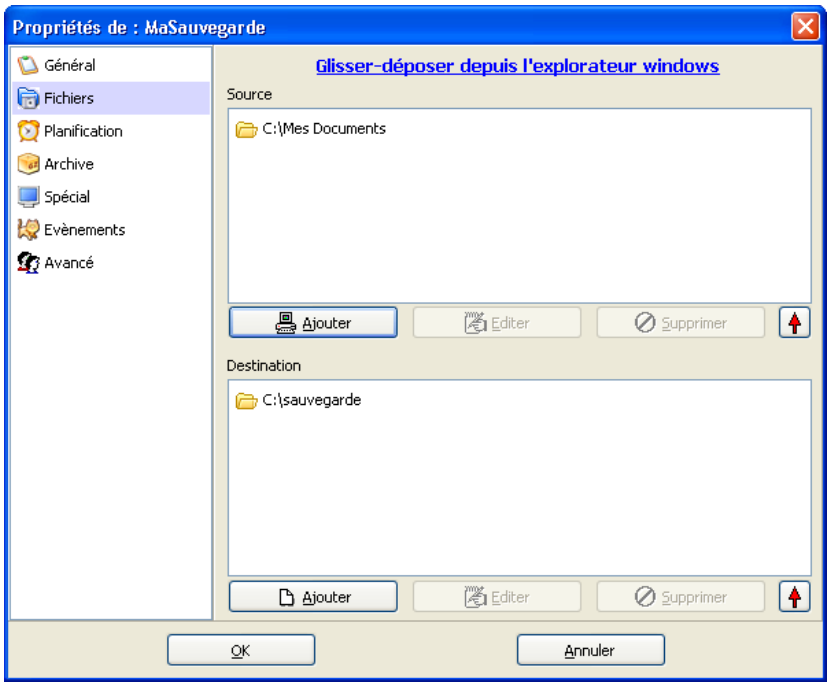


Figure 3 : La fenêtre Propriétés de : affichant les fenêtres Source et Destination

Deuxième étape. **Sélectionnez** les fichiers que vous souhaitez copier. (Dans l'exemple précédent, le dossier *Mes documents* est sélectionné.)

Troisième étape. **Cliquez** sur Ajouter dans la fenêtre **Source** pour activer le menu suivant :

Figure 4 : La fenêtre Source – le menu du bouton Ajouter

Quatrième étape. **Sélectionnez** *Fichiers* pour créer des copies de sauvegarde de fichiers individuels, et *Répertoire* si vous souhaitez créer une copie de sauvegarde d'un répertoire entier ou pour indiquer quel fichier ou répertoire doit être copié.

Commentaire : Vous pouvez ajouter autant de fichiers ou de répertoires que vous le souhaitez. Si vous souhaitez effectuez une sauvegarde de fichiers se trouvant déjà sur votre serveur FTP, **sélectionnez** l'option *Site FTP* (vous aurez besoins des détails de connexion appropriés pour vous connecter au serveur).

Après avoir sélectionné les fichiers et/ou dossiers, vous les verrez apparaître dans la zone *Source*. Comme vous le constatez avec l'exemple ci-dessous, *Mes documents* est affiché dans cette partie, ce qui veut dire que ce dossier fait maintenant partie de la copie de sauvegarde.

La fenêtre *Destination* désigne l'endroit où les copies de sauvegarde seront stockées.

Cinquième étape. **Cliquez** sur : Ajouter dans la fenêtre *Destination* pour activer le menu suivant :

Figure 5 : La fenêtre Destination – le menu du bouton Ajouter

Sixième étape. **Sélectionnez** *Répertoire*. Une fenêtre de navigation s'ouvre par laquelle vous devez sélectionner le répertoire de destination de votre copie de sauvegarde.

Commentaire : Si vous souhaitez créer différentes versions de la copie de sauvegarde du fichier, vous pouvez à ce moment sélectionner plusieurs répertoires. Si vous avez coché l'option *Manuellement*, vous devez saisir le chemin complet vers le répertoire où vous souhaitez conserver la copie de sauvegarde. Pour utiliser un serveur Internet distant pour stocker votre archive, **sélectionnez** l'option *Site FTP* (vous aurez besoins des détails de connexion appropriés pour vous connecter au serveur).

La fenêtre devrait maintenant ressembler à l'exemple ci-dessus, avec des fichiers et/ou des répertoires dans la zone source et des répertoires dans la zone destination. Toutefois, ne cliquez pas tout de suite sur *OK*! Nous devons encore planifier la création de nos copies de sauvegarde!

2.4 Comment planifier vos tâches de sauvegarde

La dernière partie que nous devons aborder afin que nos copies de sauvegarde automatiques soient fonctionnelles est la partie *Planification*. Cette partie vous permet de déterminer les moments où vous souhaitez que vos copies de sauvegarde soient créées.

Pour régler les options de planification, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez** *Planification*, dans le menu de gauche, pour activer la fenêtre suivante :

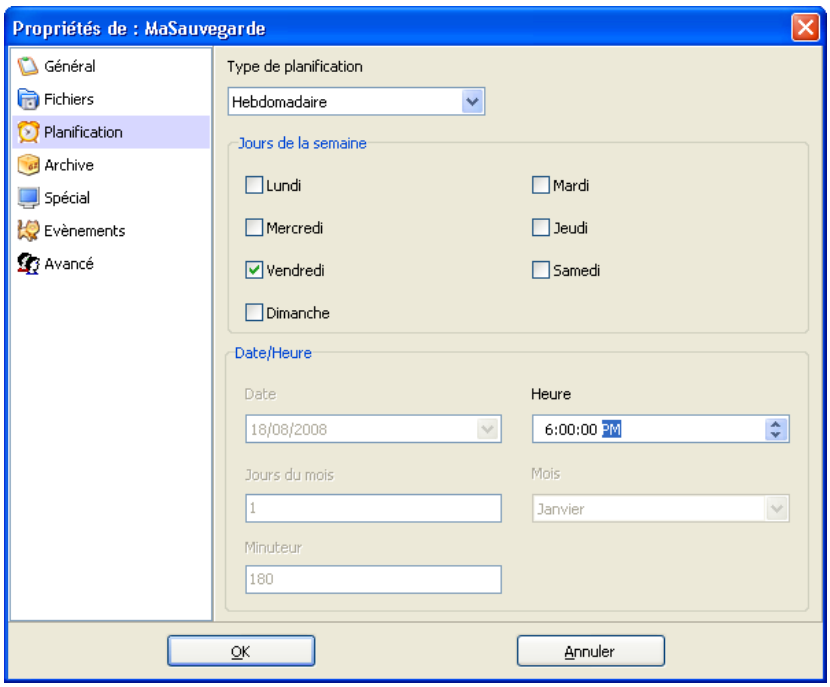


Figure 6 : Les Propriétés de MaSauvegarde affichant la fenêtre Type de planification.

Les options de *Type de planification* sont énumérées dans un menu défilant. Elles sont décrites ci-dessous :

Une fois : La copie de sauvegarde sera créée une seule fois à la date et à l'heure que vous inscrivez dans la zone *Date/Heure*.

Quotidienne : La copie de sauvegarde sera créée chaque jour à la date et à l'heure que vous inscrivez dans la zone *Date/Heure*.

Hebdomadaire : La copie de sauvegarde sera créée le jour de la semaine que vous aurez choisi. Dans l'exemple ci-dessus, la copie est créée le vendredi. Vous pouvez aussi choisir une autre journée. La copie de sauvegarde sera créée selon les journées et l'heure inscrites dans la zone *Date/Heure*.

Mensuelle : La copie de sauvegarde sera créée selon les journées choisies dans la boîte *mois* à l'heure inscrite dans la zone *Date/Heure*.

Annuelle : La copie de sauvegarde sera créée selon les journées choisies dans la boîte *mois*, au cours du mois que vous aurez également choisi et à l'heure inscrite dans la zone *Date/Heure*.

Minuterie : La copie de sauvegarde sera créée à plusieurs reprises aux intervalles inscrits dans la boîte *Minuteur* de la zone *Date/Heure*.

Manuellement : Vous devrez exécuter la copie vous-même depuis la fenêtre principale du programme.

Deuxième étape. **Cliquez** sur le bouton *OK*.

La planification des sauvegardes clôt le processus. Des copies de sauvegarde des fichiers sélectionnés seront désormais créées aux moments que vous avez déterminés.

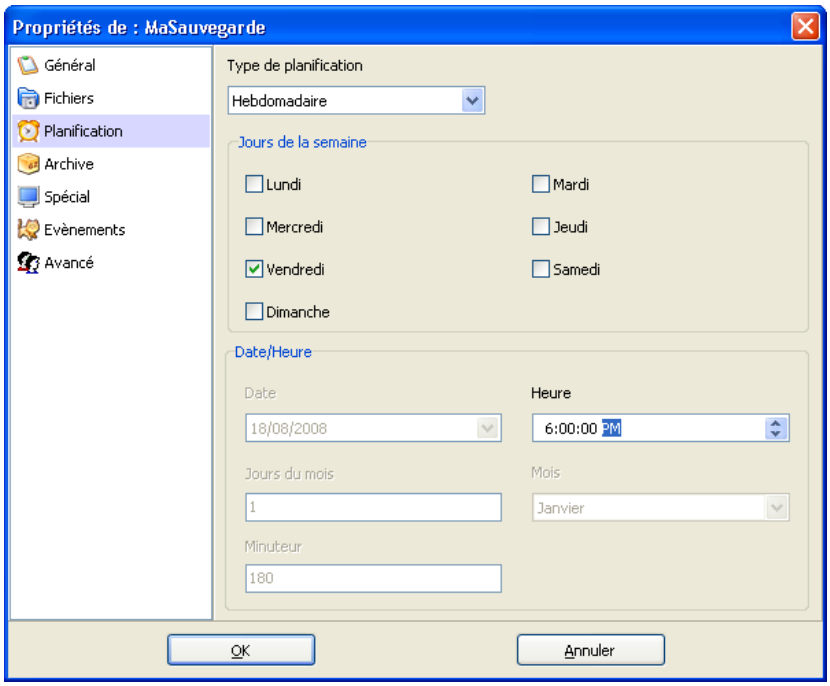


Figure 7 : Les propriétés de MaSauvegarde affichant le panneau Type de planification

Compresser vos archives

Étape 1. Créez une tâche de sauvegarde pour tous les fichiers que vous souhaitez archiver en suivant les étapes énumérées à la section **2.3 Créer une copie de sauvegarde** [86].

Étape 2. Sélectionnez l'option *Archive* dans le menu de gauche pour activer la fenêtre *Propriétés de:*

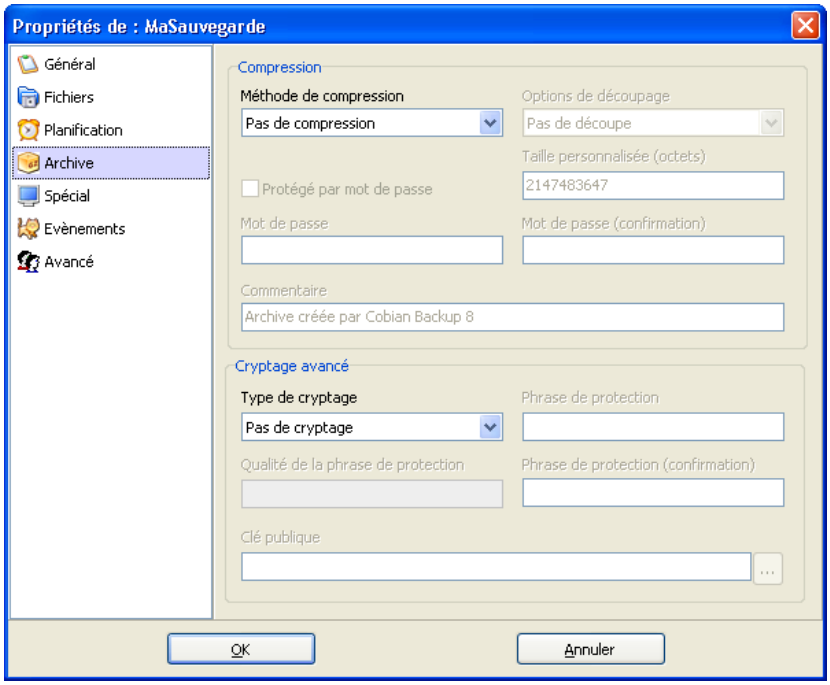


Figure 8 : La fenêtre Propriétés de: affichant les rubriques Compression et Cryptage avancé

3.1 Comment compresser vos archives

La rubrique *Compression* sert à déterminer la méthode de compression de votre choix.

La compression sert à réduire l'espace employé pour stocké vos fichiers. Supposons que votre ordinateur contienne une série de vieux fichiers dont vous vous servez peu, mais que vous souhaitez tout de même conserver. Il est logique que vous les stockiez dans un format qui occupe le moins d'espace possible en ayant recours aux techniques de compression et de décompression. La compression enlève les éléments de codification peu importants d'un document, tout en conservant l'information importante. La compression n'abîme pas vos données originales. Les fichiers ne sont pas visibles lorsque compressés. Le processus inverse, la *décompression*, doit être appliqué aux fichiers pour les rendre visibles à nouveau.

Les trois sous-options du menu défilant de la *méthode de compression* sont :

Pas de compression : Tel que son nom l'indique, cette option n'exécute pas de compression.

Compression Zip : Il s'agit de la technique de compression normale pour les systèmes **Windows**. Les archives, une fois

créées, peuvent être ouvertes à l'aide des outils Windows habituels (vous pouvez aussi télécharger le programme ZipGenius [87] pour les ouvrir). Cette option est la plus pratique des trois.

Compression SQX : La compression SQX est plus lente que la compression Zip. Cependant, en cas de corruption des archives, son taux de récupération des données est plus élevé.

Si vous avez choisi l'une des trois options de compression mentionnées ci-dessus, vous pouvez également choisir :

Options de découpage, du menu défilant. Cette option est pratique pour stocker des données sur des supports portatifs comme des CD, des DVD, des disquettes ou des clés USB. Vos archives seront découpées en morceaux dont la taille correspond au dispositif de stockage de votre choix. Supposons que vous copiez un grand nombre de fichiers, que vous souhaitez les transférer sur un CD et que la taille de vos archives dépasse 700 Mo (la taille d'un CD). La fonction de découpage divisera vos archives en morceaux plus petits que 700 Mo, ou équivalents à cette taille : vous pourrez alors les graver sur un ou plusieurs CD. Si vous prévoyez créer des copies de sauvegarde du disque dur de votre ordinateur ou que la taille de votre copie de sauvegarde est inférieure à la capacité de stockage de votre dispositif, vous pouvez passer cette section.

Les options de taille suivantes vous sont offertes lorsque vous cliquez sur le menu défilant *Options de découpage*. Votre choix dépendra du dispositif de stockage que vous souhaitez utiliser.

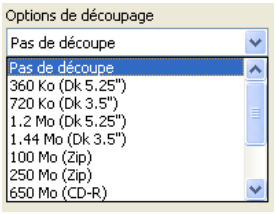


Figure 9 : Le menu défilant Options de découpage

- 3,5" – Disquette. Cette option contient assez d'espace pour y stocker un petit nombre de documents.
- Zip – Disque Zip (vérifiez la capacité du disque Zip que vous utilisez). Vous aurez besoin d'un lecteur de disque Zip connecté à votre ordinateur et des disques personnalisés.
- Disque CD-R – CD (vérifiez la capacité du disque que vous utilisez). Vous aurez besoin d'un graveur de CD connecté à votre ordinateur et d'un programme d'écriture de CD.
- Disque DVD – DVD (vérifiez la capacité du disque que vous utilisez). Vous aurez besoin d'un graveur DVD connecté à votre ordinateur et d'un programme d'écriture DVD.

Si vous créez des copies de sauvegarde que vous stockez sur plusieurs clés USB, vous avez peut-être intérêt à fixer une taille personnalisée.

Pour ce faire, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez** l'option *Taille personnalisée*, et **saisissez** la taille de l'archive en octets dans la zone de texte :

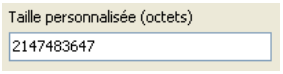


Figure 10 : La zone de texte Taille personnalisée

Un aperçu des tailles :

- 1 Ko (kilooctet) = 1 024 octets – un document texte d'une page fait à l'aide de Open Office correspond environ à 20 Ko.
- 1 Mo (mégaoctet) = 1 024 Ko – une photo prise à l'aide d'une caméra numérique se situe généralement entre 1 et 3 Mo.
- 1 Go (gigaoctet) = 1 024 Mo – environ une demi-heure d'un film DVD de bonne qualité.

Commentaire : Lorsque vous choisissez une taille personnalisée pour découper vos copies de sauvegarde afin de les stocker sur un DVD ou un CD, Cobian Backup ne copiera pas automatiquement la sauvegarde sur votre dispositif de stockage. Le programme créera plutôt vos archives sur votre ordinateur, et vous devrez les graver vous-même sur le CD ou le DVD.

Protéger par mot de passe : Cette option vous permet de choisir un mot de passe pour protéger vos archives. Saisissez simplement, deux fois, un mot de passe dans les zones de texte appropriées. Au moment de décompresser l'archive, le programme vous demandera votre mot de passe avant d'exécuter la tâche.

Commentaire : Si vous souhaitez augmenter le niveau de sécurité de l'archive, vous devriez envisager d'utiliser une autre méthode que celle du mot de passe. Cobian Backup vous permet également de chiffrer votre archive. Cette méthode sera abordée dans la section qui suit, **4. Chiffrer vos archives** [88]. Sinon, vous pouvez aussi consulter le Guide pratique TrueCrypt [89] pour apprendre comment créer un volume de stockage chiffré sur votre ordinateur ou sur un dispositif amovible.

Commentaire : Cette option vous permet d'inscrire une information descriptive au sujet de l'archive (facultatif).

3.2 Comment décompresser votre archive

Pour décompresser votre archive, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez : Outils > Décompacteur**

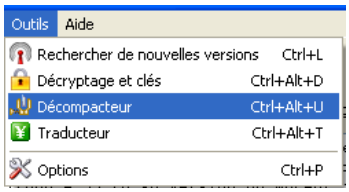


Figure 16 : Le menu Outils affichant l'option Décompacteur

La fenêtre *Décompacteur* apparaît :

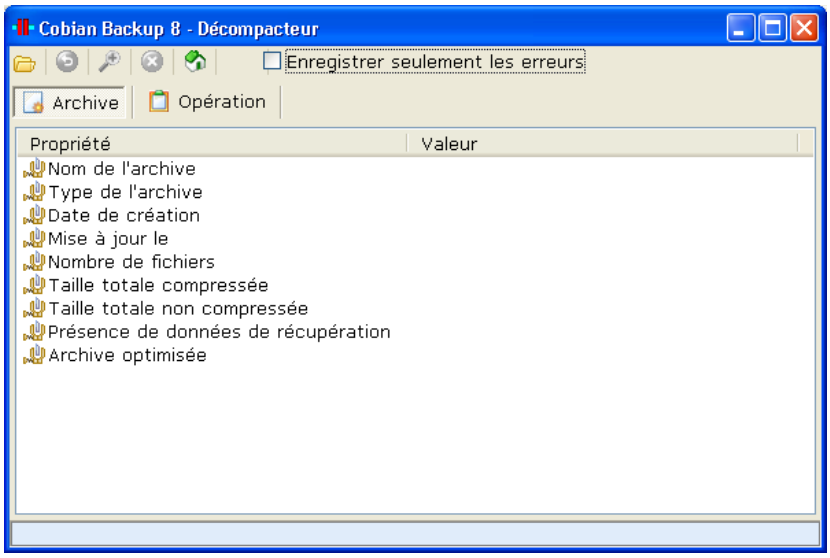


Figure 17 : La fenêtre Cobian Backup - Décompacteur

Deuxième étape. **Cliquez** sur :

Troisième étape. **Sélectionnez** l'archive (fichier .zip ou .sqx)

Quatrième étape. **Cliquez** sur le bouton *OK*.

Cinquième étape. **Sélectionnez** un répertoire ou vous souhaitez décompresser le fichier archivé.

Sixième étape. **Cliquez sur** :

Vous verrez apparaître une nouvelle fenêtre qui vous permettra de choisir le répertoire où vous souhaitez décompresser l'archive.

Septième étape. **Sélectionnez** un répertoire.

Huitième étape. **Cliquez** sur le bouton *OK*.

Utilisez **Windows Explorer** pour voir les fichiers transférés dans ce répertoire.

Chiffrer vos archives

Le chiffrement peut s'avérer nécessaire si vous voulez protéger vos copies de sauvegarde des accès non autorisés. Le *Chiffrement* est le processus de codification, ou d'embrouillage, des données : une fois chiffrées, les données sont inintelligibles pour quiconque ne détient pas la clé nécessaire au décodage du message. Pour plus de renseignements sur le chiffrement, veuillez consulter le chapitre 4. Protéger les données sensibles stockées sur votre ordinateur [90] du livret pratique.

4.1 Comment chiffrer vos archives

La fenêtre *Cryptage avancé* sert à préciser la méthode de chiffrement que vous souhaitez utiliser.

Étape 1 : **Cliquez** sur le menu défilant *Type de cryptage* pour activer la liste des diverses méthodes de chiffrement :

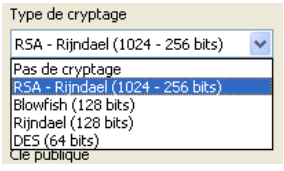


Figure 11 : Le menu défilant des types de chiffrement

Par souci de simplicité, nous vous recommandons de choisir entre les méthodes *Blowfish* et *Rijndael* (128 octets). Ces méthodes sont très sûres et vous permettent d'accéder aux données chiffrées à l'aide d'une phrase de protection que vous choisissez.

Deuxième étape: **Sélectionnez** le *type de chiffrement* de votre choix.

Commentaire : *Rijndael* et *Blowfish* s'équivalent en ce qui concerne le niveau de sécurité. *DES* est plus faible, mais le processus de chiffrement est plus rapide.

Troisième étape : **Saisissez** (deux fois) la phrase de protection dans les boîtes appropriées, tel que dans l'exemple suivant :

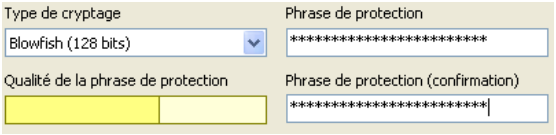


Figure 12 : Les zones de texte du Type de chiffrement et de la phrase de protection

La force de la phrase de protection est indiquée par la barre *Qualité de la phrase de protection*. Plus la barre bouge vers la droite, plus la phrase de protection est forte. Voir le chapitre 3. Créer et sauvegarder des mots de passe sûrs du livret pratique pour obtenir des directives sur la création et le stockage de mots de passe sûrs.

Quatrième étape : **Cliquez** sur le bouton *OK*.

4.2 Comment déchiffrer votre archive

Étape 2. **Sélectionnez** : **Outils > Décryptage et clés**

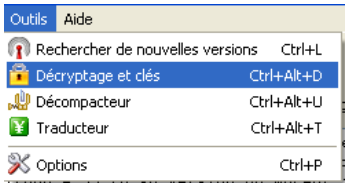


Figure 13 : Le menu Outils avec l'option Décryptage et Clés sélectionnée

Ceci activera la fenêtre *Décryptage et clés* :

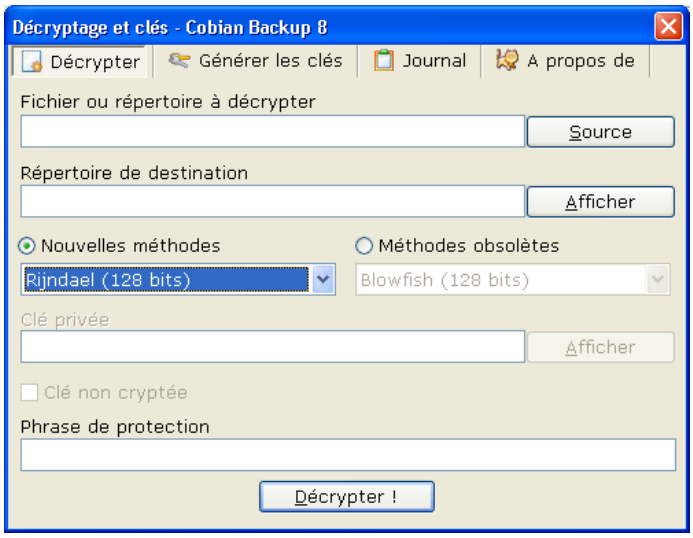


Figure 14 : La fenêtre Décryptage et Clés dans Cobian Backup 8

Deuxième étape. **Cliquez** sur le bouton *Source* pour sélectionner l'archive que vous souhaitez déchiffrer.

Troisième étape. **Cliquez** sur le bouton *Afficher* pour sélectionner le répertoire où l'archive doit être stockée.

Quatrième étape. **Sélectionnez** le type de chiffrement (que vous avez choisi à la section **4.1 Comment chiffrer vos archives**) dans le menu défilant *Nouvelles méthodes.*

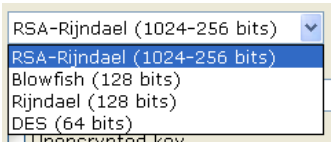


Figure 15 : Le menu défilant Nouvelles méthodes

Cinquième étape. **Sélectionnez** la méthode de chiffrement appropriée (celle que vous avez utilisée pour chiffrer votre copie de sauvegarde).

Sixième étape. **Saisissez** votre *Phrase de protection* dans la zone de texte du même nom.

Septième étape. **Cliquez** sur le bouton *Décrypter*.

Les fichiers seront déchiffrés vers l'emplacement que vous avez spécifié. Si les fichiers étaient également compressés, vous

devrez les décompresser en suivant les étapes énumérées à la section **3.2 Comment décompresser vos archives**. [91]

Faq et questions récapitulatives

Elena et Nikolai savent à quel point il est important de créer des copies de sauvegarde de leurs documents : ils ont déjà perdu des fichiers importants suite au bris d'un ordinateur causé par un virus. **Cobian Backup** est une solution adéquate au problème de rationalisation du processus de création de copies de sauvegarde, bien que l'on doive prendre un peu de temps pour l'installer et s'y habituer.

Elena, après avoir appris à s'en servir, est heureuse d'utiliser la fonction de base de création de copies de sauvegarde. Elle sait qu'elle peut conserver ses copies dans un emplacement sûr, loin de son ordinateur et de son bureau. De plus, elle trouve que la fonction de compression des fichiers de sauvegarde est très utile puisqu'elle permet d'économiser de l'espace sur son ordinateur. Nikolai est particulièrement content de pouvoir utiliser un seul programme pour à la fois chiffrer un document d'archive et en créer une copie de sauvegarde. Il est aussi intéressé à approfondir l'option *Sauvegarder sur un serveur distant par ftp* dans un avenir rapproché, afin de pouvoir stocker des copies de fichiers importants sur des serveurs qui se trouvent ailleurs dans le monde.

Toutefois, Elena et Nikolai ont tous deux quelques questions au sujet de Cobian Backup :

Q. : *Si je conserve les archives de mes fichiers sur un DVD, est-ce que je peux décompresser et déchiffrer mes fichiers sur un autre ordinateur que le mien? Est-ce possible de les utiliser dans un café Internet?*

R. : *Tu peux restaurer ton archive, qu'elle soit chiffrée ou compressée, sur n'importe quel ordinateur où Cobian Backup est installé.*

Q. : *Je suis aux prises avec un véritable problème d'espace sur mon ordinateur. J'ai des doutes quant à l'espace que je pourrai économiser en compressant mes fichiers. Peux-tu me donner quelques exemples simples?*

R. : *La majeure partie de l'espace d'un ordinateur est habituellement occupée par des fichiers photos, vidéo et audio. Tu peux vérifier l'espace que ces fichiers occupent sur ton ordinateur en cliquant à droite sur le répertoire qui les contient et en choisissant l'option Propriétés. Si tu as peu d'espace libre sur ton ordinateur, tu peux envisager de créer des archives des fichiers pour ensuite retirer les originaux de ton ordinateur.*

Q. : *On me demande toujours de mettre à jour des programmes que j'obtiens sur Internet. Si une nouvelle version de Cobian Backup est créée et que je la télécharge, j'ai peur de ne plus avoir accès à mes fichiers compressés et chiffrés. Devrais-je télécharger des mises à jour?*

R. : *Tu devrais toujours télécharger les plus récentes mises à jour, puisqu'elles apportent souvent des améliorations opérationnelles et sécuritaires. Cobian Backup continuera de bien fonctionner sur ton ordinateur, et toutes les nouvelles versions seront compatibles avec les copies créées avec une ancienne version du programme.*

Q. : *La présence de ce programme sur mon ordinateur ne signale-t-elle pas clairement que j'ai des données chiffrées?*

R. : *Tu n'as pas besoin de conserver une copie de sauvegarde chiffrée sur ton ordinateur. Cobian Backup n'est pas un programme réputé pour le chiffrage de données, puisque ce n'est pas sa fonction principale.*

Q. : *Est-ce préférable d'utiliser Cobian Backup ou* **TrueCrypt** *pour chiffrer des fichiers ?*

R. : *Il est préférable d'utiliser TrueCrypt pour chiffrer des fichiers sur ton ordinateur. Le mécanisme de chiffrage est plus puissant et offre la possibilité d'ajouter et de supprimer des fichiers du volume chiffré. Tu peux par ailleurs créer une copie de sauvegarde d'un volume TrueCrypt à l'aide de Cobian Backup.*

Q. : *Y a-t-il d'autre information que je dois connaître avant d'installer l'option de* Sauvegarde sur serveur distant par FTP*?*

R. : *Tu devrais savoir si ton fournisseur offre le service **FTP**, et connaître les détails d'ouverture de session. Il est préférable que tu utilises une version sécurisée de FTP, le **SFTP**, si cette option est offerte par ton fournisseur de service.*

4.1 Questions récapitulatives

1. Quelle est la différence entre les copies de sauvegarde incrémentielles et différentielles ?
2. Quelle est la meilleure façon de sécuriser une copie de sauvegarde?
3. Comment stocker une copie de 1 Go sur un disque CD?
4. Comment restaurer un seul fichier d'une copie de sauvegarde?
5. Est-il possible de créer une tâche automatisée de sorte que votre ordinateur mette à jour les copies de sauvegarde une fois par semaine, le vendredi après-midi? Quelles sont les étapes à suivre pour y arriver ?

Recuva - récupération de fichiers

Short Description:

Recuva est un outil facile à utiliser qui permet de récupérer des fichiers perdus. Vous pouvez scanner vos disques pour récupérer des documents, fichiers, dossiers ou autres données, y compris des messages de courrier électronique, des images et des clips vidéo. **Recuva** emploie également des techniques d'écrasement sécurisées pour effacer des données sensibles et/ou privées.

Online Installation Instructions:

Pour installer Recuva

- *Lisez la courte introduction des **Guides pratiques** [1]*
- ***Cliquez** sur l'icone **Recuva** ci-dessous pour afficher la page de téléchargement **www.piriform.com/recuva/builds***
- *Dans la section 'Recuva - Slim', **cliquez** sur le bouton 'Download'*
- ***Sauvegardez** le fichier exécutable 'rcsetup_slim.exe' sur votre ordinateur, puis **double-cliquez** dessus pour lancer l'installation du programme*

- *Lisez attentivement les 'consignes d'installation' détaillées à la prochaine section avant de continuer*
- *Après avoir complété l'installation de **Recuva** vous pouvez supprimer l'exécutable d'installation de votre ordinateur*

Recuva:

[92]

Site Internet

www.piriform.com/recuva [93]

Configuration requise

- Compatible avec toutes les versions de Windows (**Commentaire**: Le soutien technique pour **Windows 98** n'est plus disponible.)

Version utilisée pour rédiger ce guide

- 1.3

Licence

- Gratuiciel

Lecture requise

- Livret pratique Security in-a-box, chapitre **5. Récupérer des données perdues** [94]

Niveau: 1: Débutant, **2: Moyen**, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 20 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité d'exécuter différentes méthodes de scan
- La capacité de récupérer des fichiers préalablement supprimés de votre ordinateur
- La capacité d'effacer de façon sécurisée certaines données privées ou sensibles

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Pour les utilisateurs **GNU Linux**, nous recommandons **R-Linux** [95].
Les utilisateurs de **Mac OS** apprécieront sans doute **TestDisk** et **PhotoRec** [96], qui sont également compatibles avec **Microsoft Windows** et **GNU Linux**.
À part **Recuva**, il existe d'autres programmes de récupération de données compatibles avec **Microsoft Windows**:

- **NTFS Undelete** [97]
- **Disk Digger** [98]
- **PCInspector File Recovery** [99]
- **Undelete Plus** [100]

1.1 À propos de cet outil

Dans les situations fâcheuses où certaines données sensibles auraient pu être supprimées par accident, **Recuva** peut vous aider à les restaurer. Comme nous l'avons vu au chapitre **6. Détruire définitivement des données sensibles** [37], un fichier supprimé à l'aide de la méthode de suppression standard du système **Windows**, même après que la *corbeille* eut été vidée, existe peut-être toujours quelque part sur le disque dur.

Il existe tout de même certaines circonstances où **Recuva** n'est pas en mesure de retrouver les données. Si vous avez *effacé*, ou supprimé de façon permanente, des fichiers temporaires à l'aide de **CCleaner** et de sa fonction *Effacement sécurisé (Lent)*, ces fichiers sont irrécupérables. **Recuva** ne peut pas récupérer des fichiers après que des programmes comme **CCleaner** ou **Eraser** aient été utilisés pour effacer l'espace libre de vos disques durs, ou après que *Windows* ait écrasé lesdits fichiers avec de nouvelles données. De plus, **Recuva** ne peut pas récupérer des fichiers ou documents endommagés.

Recuva peut également être utilisé pour écraser de façon sécuritaire des données privées ou sensibles.

Comment installer Recuva

2.0 Comment installer Recuva

L'installation de **Recuva** est relativement simple et rapide. Pour lancer l'installation de **Recuva**, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** sur rcsetup138_slim ; Il est possible que s'ouvre une boîte de dialogue *Fichier ouvert - Avertissement de sécurité*. Si c'est le cas, **cliquez** sur Exécuter pour afficher la boîte de dialogue suivante:

Figure 1: La boîte de sélection de la langue de l'assistant

Deuxième étape. **Cliquez** sur OK pour afficher l'*Assistant d'installation de Recuva*.

Troisième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Licence utilisateur*. Veuillez lire attentivement la *Licence Utilisateur* avant de poursuivre le processus d'installation.

Quatrième étape. **Cliquez** sur J'accepte.

Cinquième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Options d'installation*.

Commentaire: Selon la version, il est possible que la fenêtre *Options d'installation* s'affiche avec l'option *Install optional Yahoo! toolbar* sélectionnée par défaut. Si c'est le cas, dessélectionnez cette option parce qu'elle pourrait compromettre votre confidentialité sur Internet. (NDT: Dans la version v1.38, cette option a été éliminée du processus d'installation.)

Sixième étape. **Dessélectionnez** l'option *Install optional Yahoo! toolbar*.

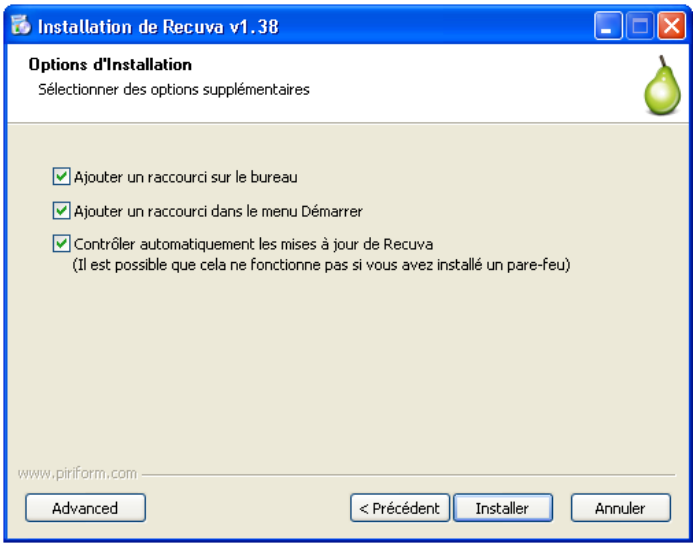

Installation de Recuva v1.38
Options d'Installation
Sélectionner des options supplémentaires
Ajouter un raccourci sur le bureau
Ajouter un raccourci dans le menu Démarrer
Contrôler automatiquement les mises à jour de Recuva
(Il est possible que cela ne fonctionne pas si vous avez installé un pare-feu)
www.piriform.com
Advanced
< Précédent
Installer
Annuler

Figure 2: La fenêtre Options d'installation

Septième étape. **Cliquez** sur Installer pour lancer l'installation de **Recuva**. La barre de progression de l'installation s'affichera momentanément, puis l'installation se complètera d'elle même en quelques minutes.

Huitième étape. ***Cliquez** sur Fermer pour finaliser l'installation de **Recuva**.

Maintenant que vous avez finalisé l'installation de **Recuva**, vous êtes prêt à récupérer et/ou écraser des données privées ou sensibles. Pour ce faire, veuillez lire attentivement la section **3.0 Comment exécuter différents types de scan avec Recuva** [101].

Comment exécuter différents types de scan avec Recuva

Sommaire des sections de cette page:

- **3.0 Avant de commencer**
- **3.1 Comment exécuter un scan avec l'assistant de Recuva**
- **3.2 Comment exécuter un scan sans utiliser l'assistant de Recuva**
- **3.3 Comment exécuter une Analyse approfondie avec Recuva**
- **3.4 Une introduction à la fenêtre Options**

3.0 Avant de commencer

Dans cette section, nous verrons comment lancer différent types de scans et nous examinerons les onglets *Général* et *Actions* de la fenêtre *Options*.

Commentaire: Un scan ne fait que retrouver et afficher les fichiers récupérables. Le processus de récupération comme tel sera examiné à la section **4.0 Comment récupérer et effacer des fichiers de façon sécuritaire avec Recuva** [102].

3.1 Comment exécuter un scan avec l'assistant de Recuva

L'*Assistant* de **Recuva** est recommandé dans les situations ou le nom du fichier à récupérer n'est pas connu. Ce mode est également recommandé si vous utilisez **Recuva** pour la première fois. L'*Assistant* de **Recuva** vous laisse régler les paramètres du scan en vous permettant de spécifier le type de fichier et/ou l'emplacement original du fichier supprimé.

Pour commencer à chercher les fichiers supprimés, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur ou **sélectionnez Démarrer > Programmes > Recuva > Recuva** pour lancer le programme et afficher la fenêtre suivante:

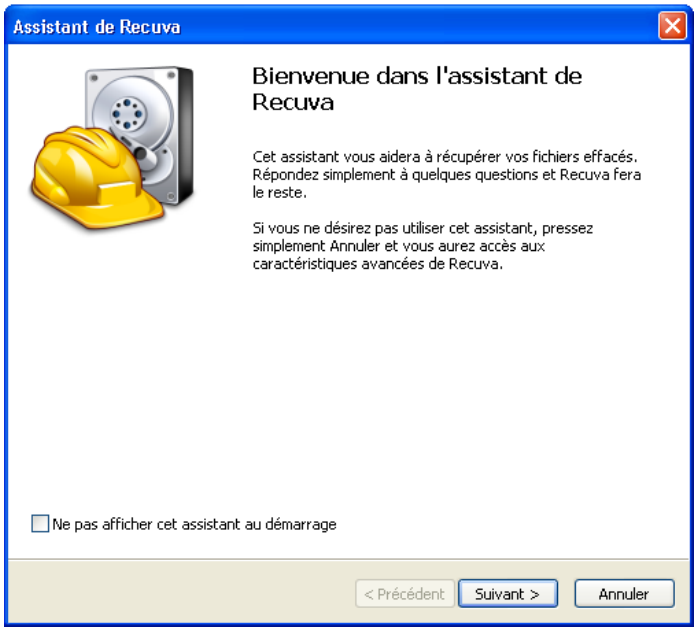

Assistant de Recuva
Bienvenue dans l'assistant de Recuva
Cet assistant vous aidera à récupérer vos fichiers effacés. Répondez simplement à quelques questions et Recuva fera le reste.
Si vous ne désirez pas utiliser cet assistant, pressez simplement Annuler et vous aurez accès aux caractéristiques avancées de Recuva.
Ne pas afficher cet assistant au démarrage
< Précédent
Suivant >
Annuler

Figure 1: La fenêtre Bienvenue dans l'assistant de Recuva

Astuce: Si vous connaissez le nom du fichier que vous souhaitez récupérer, au complet ou en partie, **cliquez** sur Annuler pour vous afficher l'interface principale de *Piriform Recuva*. Vous n'avez ensuite qu'à suivre les consignes décrites à la section **3.2 Comment exécuter un scan sans utiliser l'assistant de Recuva**.

Deuxième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

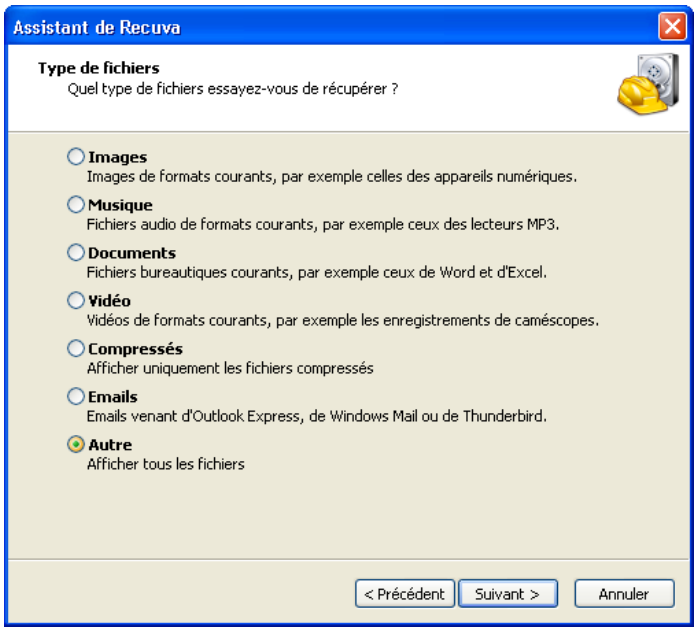

Assistant de Recuva
Type de fichiers
Quel type de fichiers essayez-vous de récupérer ?
Images
Images de formats courants, par exemple celles des appareils numériques.
Musique
Fichiers audio de formats courants, par exemple ceux des lecteurs MP3.
Documents
Fichiers bureautiques courants, par exemple ceux de Word et d'Excel.
Vidéo
Vidéos de formats courants, par exemple les enregistrements de caméscopes.
Compressés
Afficher uniquement les fichiers compressés
Emails
Emails venant d'Outlook Express, de Windows Mail ou de Thunderbird.
Autre
Afficher tous les fichiers
< Précédent
Suivant >
Annuler

Figure 2: La fenêtre Type de fichiers de l'assistant de Recuva

La fenêtre *Type de fichiers* affiche une liste des différents types de fichiers et décrit quels fichiers peuvent être récupérés lorsque l'une ou l'autre des options est sélectionnée.

Troisième étape. **Cochez** l'option *autre*, tel qu'illustré à la *Figure 2*, puis **cliquez** sur Suivant > pour afficher la fenêtre suivante:

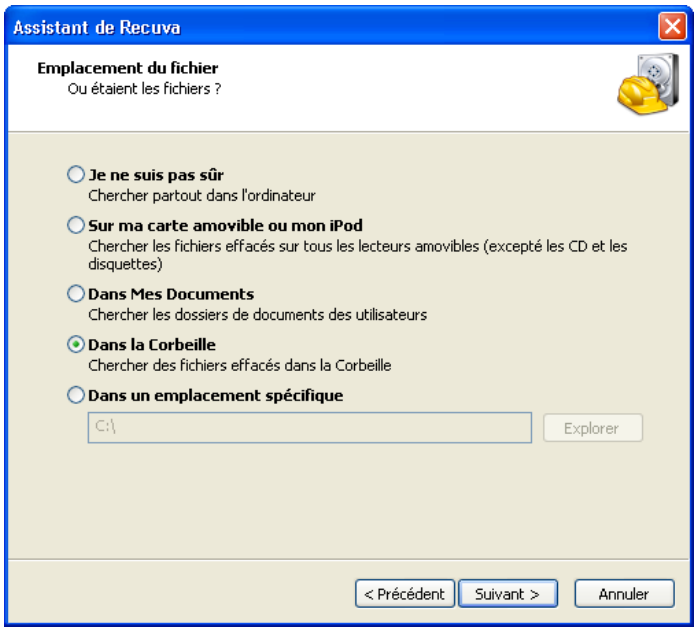

Assistant de Recuva
Emplacement du fichier
Ou étaient les fichiers ?
Je ne suis pas sûr
Chercher partout dans l'ordinateur
Sur ma carte amovible ou mon iPod
Chercher les fichiers effacés sur tous les lecteurs amovibles (excepté les CD et les disquettes)
Dans Mes Documents
Chercher les dossiers de documents des utilisateurs
Dans la Corbeille
Chercher des fichiers effacés dans la Corbeille
Dans un emplacement spécifique
C:\
Explorer
< Précédent
Suivant >
Annuler

Figure 3: La fenêtre Emplacement du fichier de l'Assistant de Recuva

Commentaire: Le réglage par défaut de la fenêtre *Emplacement de fichier* est *Je ne suis pas sûr*. Cette option lancera un scan sur tous les disques et sur tous les dispositifs amovibles, à l'exception des CD, DVD et médias optiques. Il est donc possible qu'un tel scan prennent un certain temps à générer des résultats.

Le plus souvent, les fichiers sont supprimés à partir de la *Corbeille* du système d'exploitation *Windows*, pour réduire les chances que vous supprimiez des données sensibles ou privées.

Quatrième étape. **Cochez** l'option *Dans la corbeille*, tel qu'illustré à la *Figure 3* ci-dessus, puis **cliquez** sur Suivant > pour afficher la fenêtre suivante:

Assistant de Recuva
Merci, maintenant Recuva est prêt à chercher vos fichiers
Après la fin de la recherche, vous verrez une liste des fichiers trouvés par Recuva. Sélectionnez simplement les fichiers que vous désirez récupérer et cliquez sur le bouton Récupérer.
Cochez cette option si l'analyse précédente a échouée dans la recherche des fichiers. Notez que cela peut prendre plus d'une heure pour les gros disques.
Activer l'analyse approfondie
Cliquez sur démarrer pour commencer la recherche
< Précédent
Démarrer
Annuler

Figure 4: Merci, maintenant Recuva est prêt à chercher vos fichiers

Commentaire: Pour les fins de cet exercice, n'activez pas l'option *Analyse approfondie*. Cette technique de scan sera abordée à la section **3.3 Comment exécuter une analyse approfondie**.

Première étape. **Cliquez** sur Démarrer pour entamer la restauration de vos fichiers supprimés.

Au cours du processus de récupération, de barre de progression s'affichent successivement. La barre de progression *Recherche des fichiers effacés sur les lecteurs* liste les fichiers supprimés. La barre de progression *Analyse du contenu du fichier* regroupe et trie les fichiers supprimés par types de fichiers et selon qu'ils sont récupérables ou non. Elle affiche également la durée estimée du processus de scan et d'analyse. L'interface principale de *Piriform Recuva* ressemblera alors à ceci:

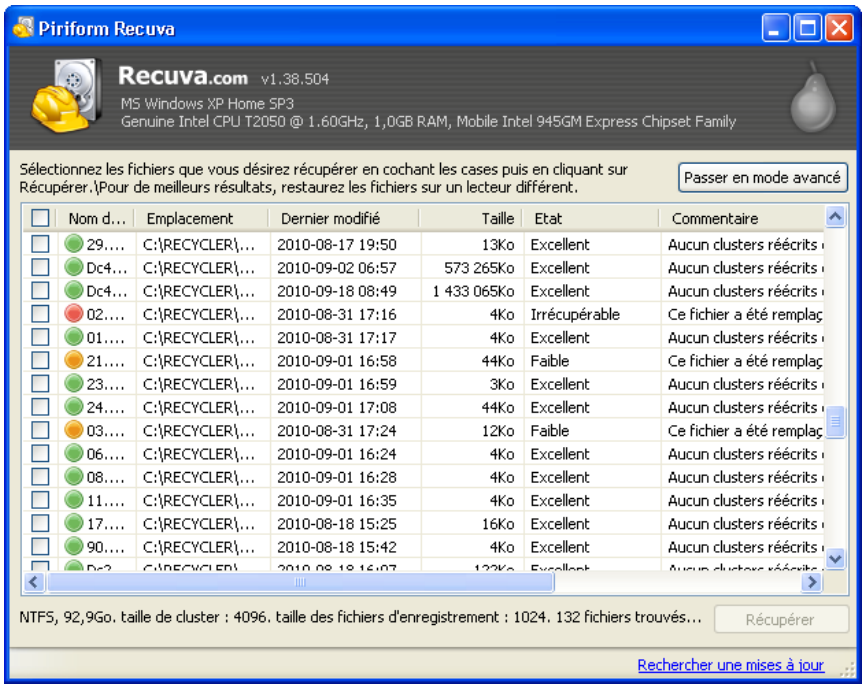

Piriform Recuva
Recuva.com v1.38.504
MS Windows XP Home SP3
Genuine Intel CPU T2050 @ 1.60GHz, 1,0GB RAM, Mobile Intel 945GM Express Chipset Family
Sélectionnez les fichiers que vous désirez récupérer en cochant les cases puis en cliquant sur Récupérer.\Pour de meilleurs résultats, restaurez les fichiers sur un lecteur différent.
Passer en mode avancé
Nom d... Emplacement Dernier modifié Taille Etat Commentaire
29.... C:\RECYCLER\... 2010-08-17 19:50 13Ko Excellent Aucun clusters réécrits
Dc4... C:\RECYCLER\... 2010-09-02 06:57 573 265Ko Excellent Aucun clusters réécrits
Dc4... C:\RECYCLER\... 2010-09-18 08:49 1 433 065Ko Excellent Aucun clusters réécrits
02.... C:\RECYCLER\... 2010-08-31 17:16 4Ko Irrécupérable Ce fichier a été remplac
01.... C:\RECYCLER\... 2010-08-31 17:17 4Ko Excellent Aucun clusters réécrits
21.... C:\RECYCLER\... 2010-09-01 16:58 44Ko Faible Ce fichier a été remplac
23.... C:\RECYCLER\... 2010-09-01 16:59 3Ko Excellent Aucun clusters réécrits
24.... C:\RECYCLER\... 2010-09-01 17:08 44Ko Excellent Aucun clusters réécrits
03.... C:\RECYCLER\... 2010-08-31 17:24 12Ko Faible Ce fichier a été remplac
06.... C:\RECYCLER\... 2010-09-01 16:24 4Ko Excellent Aucun clusters réécrits
08.... C:\RECYCLER\... 2010-09-01 16:28 4Ko Excellent Aucun clusters réécrits
11.... C:\RECYCLER\... 2010-09-01 16:35 4Ko Excellent Aucun clusters réécrits
17.... C:\RECYCLER\... 2010-08-18 15:25 16Ko Excellent Aucun clusters réécrits
90.... C:\RECYCLER\... 2010-08-18 15:42 4Ko Excellent Aucun clusters réécrits
NTFS, 92,9Go. taille de cluster : 4096. taille des fichiers d'enregistrement : 1024. 132 fichiers trouvés...
Récupérer
Rechercher une mises à jour

Figure 5: L'interface principale de Piriform Recuva affichant des fichiers supprimés retrouvés

L'interface principale de *Piriform Recuva* liste des renseignements sur chaque fichier supprimé en six colonnes. Voici une description de chaque colonne:

Nom du fichier: Cette colonne affiche le nom et l'extension de fichier du fichier supprimé **Cliquez** sur le titre *Nom du fichier*pour arranger les résultats en ordre alphabétique.

Emplacement: Cette colonne affiche l'emplacement où le fichier a été retrouvé. Puisque l'option *Dans la corbeille* a été sélectionnés dans cet exemple, l'emplacement du fichier est *C:RECYCLER* pour tous les fichiers supprimés. **Cliquez** sur le titre *Emplacement* pour afficher tous les fichiers rangés sous un emplacement de fichier ou de dossier particulier.

Dernier modifié: Cette colonne affiche la dernière date à laquelle le fichier a été modifié avant d'être supprimé. Cela peut être utile pour identifier un fichier que vous souhaiteriez récupérer. **Cliquez** le titre *Dernier modifié* pour lister les résultats du plus ancien au plus récent.

Taille: Cette colonne affiche la taille des fichiers. **Cliquez** sur *Taille* pour lister les fichiers du plus grand au plus petit, ou du plus petit au plus grand.

État: Cette colonne indique dans quelle mesure il est possible de récupérer un fichier et correspond à l'icone de l'état du fichier dont il est question à la *Figure 6* ci-dessous. **Cliquez** sur *Etat* pour trier les fichiers par catégorie, de *Excellent* à *Irrécupérable*.

Commentaire: Cette colonne affiche les raisons pour lesquelles un fichier peut ou non être récupérer, et indique si un fichier supprimé a été ou non écrasé dans la **Table de fichiers maîtres (MFT)**. **Cliquez** sur *Commentaire* pour voir dans quelle mesure un fichier ou un groupe de fichiers a été écrasé.

Chaque fichier est doté d'un icone de couleur qui indique dans quelle mesure chaque fichier peut être récupéré:

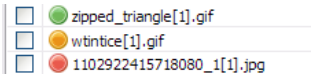


Figure 6: Les icones d'état des fichiers

La liste suivante décrit chaque icone d'état:

- **Vert**: Excellente possibilité de récupérer le fichier au complet.
- **Orange**: Possibilité acceptable de récupérer le fichier.
- **Rouge**: Très faible possibilité de récupérer le fichier.

3.2 Comment exécuter un scan sans utiliser l'assistant de Recuva

Pour accéder directement à l'interface principale de **Recuva**, c.-à-d. sans passer par l'**Assistant de Recuva**, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur

ou **sélectionnez Démarrer > Programmes > Recuva > Recuva** pour afficher la *Figure 1*.

Deuxième étape. **Cochez** l'option *Ne plus afficher cet assistant au démarrage*, puis **cliquez** sur

pour afficher la fenêtre suivante:

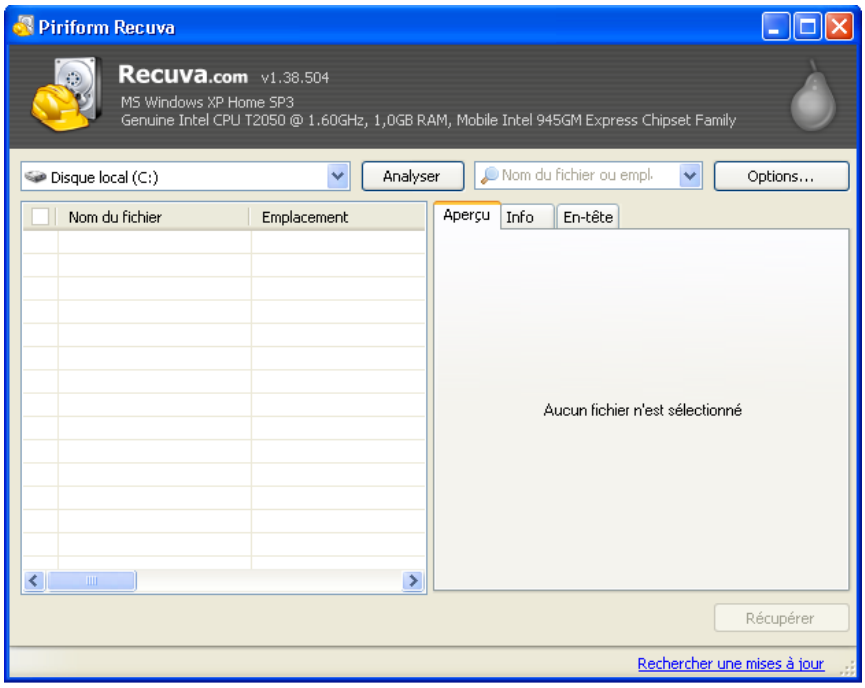


Figure 7: L'interface principale de Recuva

L'interface principale de *Piriform Recuva* est divisée en deux panneaux: le panneau des résultats, à gauche, et les onglets *Aperçu*, *Info* et *En-tête*, à droite, qui servent à trier et afficher les renseignements concernant un fichier supprimé en particulier. Vous pouvez y régler certaines options d'analyse similaires à celles qu'on retrouve dans l'*assistant de Recuva*.

Troisième étape. **Cliquez** sur le menu déroulant et **sélectionnez** le disque à analyser; le *Disque local (C:)* est sélectionné par défaut, et c'est celui qui est utilisé dans l'exemple suivant:

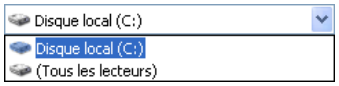


Figure 8: Le menu déroulant des disques à analyser

Le menu déroulant *Nom du fichier ou emplacement* vous permet de spécifier le type de fichier que vous recherchez, et correspond *grosso modo* aux catégories comprises dans la fenêtre *Type de fichiers de l'assistant de Recuva* illustrée à la *Figure 2*.

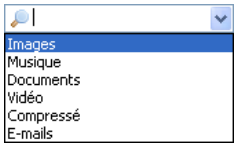


Figure 9: Le menu déroulant Nom du fichier ou emplacement

L'option *Nom du fichier ou emplacement* est une combinaison de zone de texte et de menu déroulant. Elle a deux fonctions principales: elle vous permet de chercher directement un fichier particulier, et/ou de trier un liste de fichiers supprimés par types de fichiers.

La même option l'option *Nom du fichier ou emplacement* peut être utilisée pour chercher des fichiers d'un type particulier ou de trier un liste générale de fichiers supprimés dans le panneau des résultats.

Pour retrouver un fichier dont le nom est connu (partiellement ou au complet), suivez les étapes énumérées ci-dessous:

Première étape. **Saisissez** le nom (ou la partie du nom que vous connaissez) du fichier que vous souhaitez récupérer comme suit (dans l'exemple suivant, nous cherchons le fichier *triangle.png*):

Figure 10: Le menu déroulant Nom du fichier ou emplacement affichant le nom de fichier triangle.png

Astuce: **Cliquez** sur pour rafraîchir la zone de texte *Nom du fichier ou emplacement* (qui s'affiche estompée).

Deuxième étape. **Cliquez** sur Analyser pour lancer la recherche du ou des fichier(s) supprimé(s); peu après, une fenêtre similaire à celle-ci s'affichera:

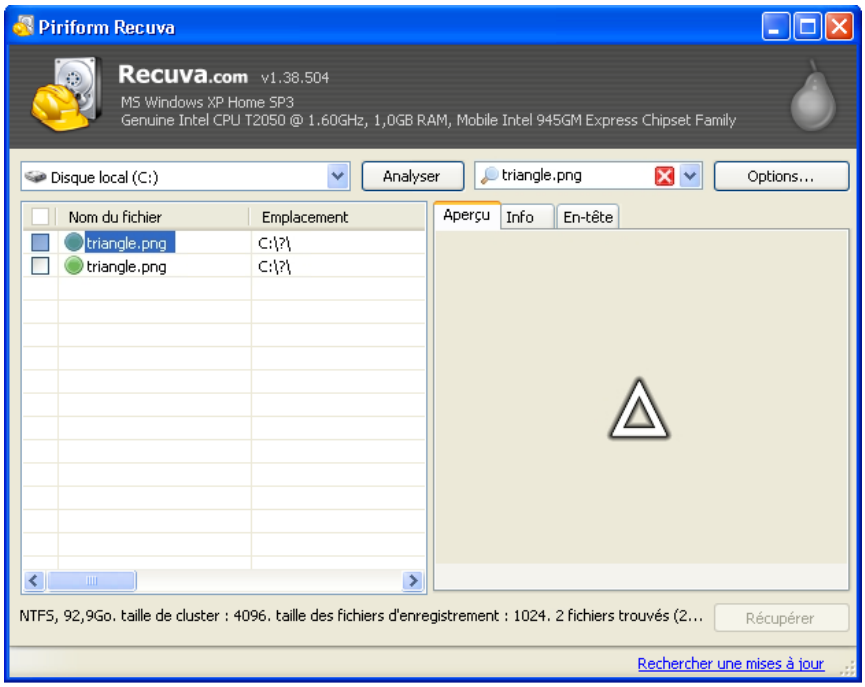
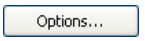


Figure 11: L'interface principale de Recuva affichant le fichier triangle.png dans l'onglet Aperçu

3.3 Comment exécuter une analyse approfondie avec Recuva

L'option *Analyse approfondie* vous permet d'exécuter un scan plus minutieux; bien entendu, une analyse approfondie prendra plus de temps, selon la vitesse de votre ordinateur et le nombre de fichiers à analyser. Cette option peut s'avérer utile si votre scan initial n'a pas trouvé les fichiers que vous souhaitez récupérer. Bien qu'une analyse approfondie puisse prendre plusieurs heures, selon la quantité de données stockées sur votre ordinateur, elle peut augmenter considérablement vos chances de récupérer les fichiers que vous cherchez.

L'option *Analyse approfondie* de **Recuva** peut également être activée en **cochant** l'option *Activer l'analyse approfondie* dans l'*assistant de Recuva* (veuillez vous référer à la *Figure 4*).

Première étape. **Cliquez** sur  pour afficher la fenêtre *Options*, puis **cliquez** sur l'onglet *Actions*:

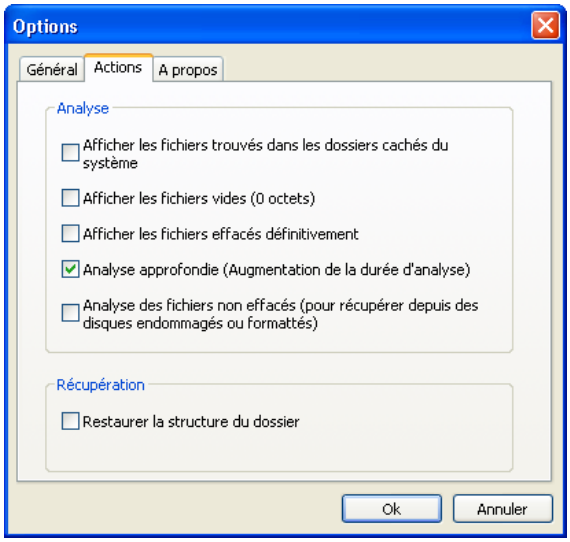
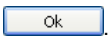
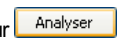


Figure 12: La fenêtre Options affichant l'onglet Actions

Deuxième étape. **Cochez** l'option *Analyse approfondie (augmentation de la durée d'analyse)*, puis **cliquez** sur  .

Troisième étape. **Cliquez** sur  pour chercher des fichiers supprimés à l'aide de la fonction *Analyse approfondie*. Il est possible que le scan prennent plusieurs heures, selon la taille du disque dur et la vitesse de l'ordinateur:

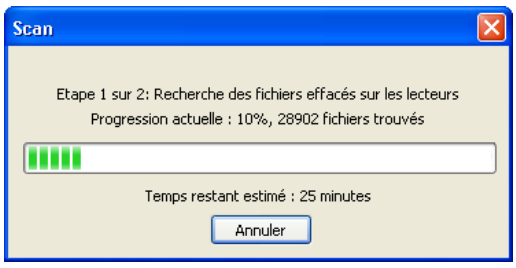

Scan
Etape 1 sur 2: Recherche des fichiers effacés sur les lecteurs
Progression actuelle : 10%, 28902 fichiers trouvés
Temps restant estimé : 25 minutes
Annuler

Figure 13: La fenêtre de progression du scan affichant le temps restant estimé pour compléter l'analyse approfondie

3.4 Une introduction à la fenêtre Options

Dans cette section, nous verrons comment utiliser les différents paramètres de la fenêtre *Options* pour récupérer et/ou écraser efficacement vos données privées ou sensibles. Pour régler ces paramètres, suivez les étapes énumérées ci-dessous:

Première étape: **Cliquez** sur

pour afficher la fenêtre suivante:

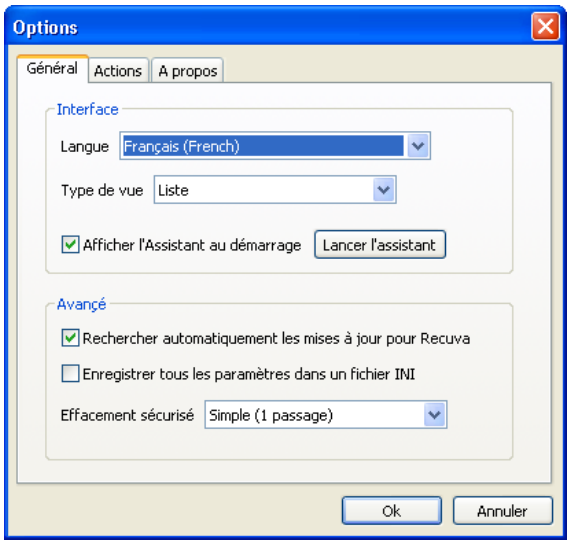


Figure 14: La fenêtre Options affichant l'onglet Général par défaut

La fenêtre *Options* est divisée en trois onglets: *Général*, *Actions* et *À propos*.

L'onglet *Général* vous permet de définir un ensemble de paramètres importants, dont la *Langue* (Recuva supporte 37 langues), le *Type de vue* et la possibilité d'activer ou de désactiver l'*Assistant de Recuva*.

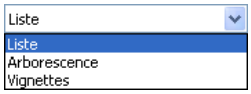


Figure 15: Le menu déroulant de l'option Type de vue

L'option **Type de vue** vous permet de choisir la façon dont s'afficheront les fichiers supprimés. Cette option peut aussi être activée en **cliquant à droite* sur un fichier dans l'interface *Piriform Recuva*.

- **Liste**: Cette option vous permet d'afficher les fichiers supprimés sous forme de liste, tel qu'illustré à la *Figure 5*.
- **Arborescence**: Cette option vous permet d'afficher l'emplacement des fichiers supprimés sous forme d'arborescence extensible.
- **Vignettes**: Cette option vous permet d'afficher les fichiers supprimés sous forme de graphiques ou d'images lorsque cela est possible.

La section *Avancé* de l'onglet *Général* vous permet de déterminer le nombre de fois que vos données seront écrasées par des données aléatoires pour empêcher que des parties malveillantes soient en mesure de les récupérer.

Le menu déroulant *Effacement sécurisé* affiche quatre options distinctes pour écraser vos données privées. Le mode par défaut est *Simple (1 passage)*, tel qu'illustré à la *Figure 14*. Les *passages* sont les fois que vos documents, fichiers ou dossiers seront écrasés avec des données aléatoires pour les rendre illisibles et irrécupérables.

Deuxième étape: **Sélectionnez** l'option *DOD 5220.22-M (3 passages)*:

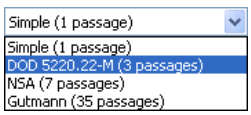
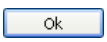


Figure 16: Le menu déroulant Effacement sécurisé avec l'option DOD 5220.22-M (3 passages) sélectionnée

Un passage simple peut être efficace pour écraser un document, un fichier ou un dossier donné; certaines personnes disposent des ressources et des capacités nécessaires pour récupérer des données relativement peu écrasées. L'option de trois passages constitue un équilibre entre la durée exigée pour écraser des données de façon sécurisée, d'une part, et la capacité de récupérer ces documents, fichiers ou dossiers, d'autre part.

Troisième étape. **Cliquez**sur 

pour sauvegarder vos paramètres de l'onglet *Général*.

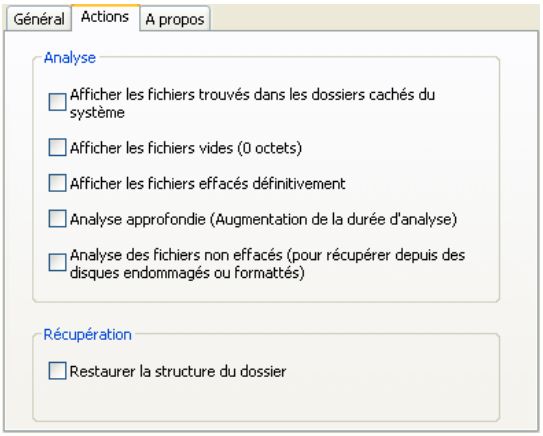

Général
Actions
A propos
Analyse
Afficher les fichiers trouvés dans les dossiers cachés du système
Afficher les fichiers vides (0 octets)
Afficher les fichiers effacés définitivement
Analyse approfondie (Augmentation de la durée d'analyse)
Analyse des fichiers non effacés (pour récupérer depuis des disques endommagés ou formattés)
Récupération
Restaurer la structure du dossier

Figure 17: La fenêtre Options affichant l'onglet Actions

- **Afficher les fichiers trouvés dans les dossiers cachés du système**: Cette option vous permet d'afficher des fichiers qui se trouvent dans des répertoires cachés du système.
- **Afficher les fichiers vides (0 octets)**: Cette option vous permet d'afficher des fichiers qui ne comportent pas ou très peu de contenu, et qui sont pratiquement irrécupérables.
- **Afficher les fichiers effacés définitivement**: Cette option vous permet d'afficher dans le panneau des résultats des fichiers qui ont été effacés de façon sécurisée.

Commentaire: Si vous avez déjà utilisé **CCleaner** ou un programme similaire, ce dernier change le nom du fichier pour *ZZZZZZZ.ZZZ* lorsqu'il efface un fichier de façon sécurisée.

- **Analyse approfondie**: Cette option vous permet de scanner un disque dur au complet pour retrouver un document ou un fichier supprimé; si les analyses précédentes n'ont pas suffit à retrouver le fichier, l'*analyse approfondie* pourrait s'avérer utile. Par contre, il faut être conscient que cette méthode prend beaucoup plus de temps. Veuillez consulter la section **3.3 Comment exécuter une analyse approfondie avec Recuva**.
- **Analyse des fichiers non effacés (pour récupérer depuis des disques endommagés ou formatés)**: Cette option vous permet d'essayer de récupérer des fichiers sur des disques qui ont subi des dommages physiques ou une corruption due à l'action de logiciels.

L'onglet *À propos* affiche des renseignements sur la version du programme, ainsi que des liens vers le site Internet de Piriform.

Maintenant que vous avez acquis la confiance nécessaire pour exécuter différents types de scans et que vous vous êtes familiarisé avec les paramètres des onglets *Général* et *Actions* de la fenêtre *Options*, nous pouvons voir comment récupérer ou effacer vos données privées ou sensibles à la section **4.0 Comment récupérer et/ou effacer des fichiers avec Recuva** [102]

Comment récupérer et/ou effacer des fichiers avec Recuva

Sommaire des sections de cette page:

- **4.0 Avant de commencer**
- **4.1 Comment récupérer un fichier supprimé**
- **4.2 Comment utiliser le menu contextuel**
- **4.3 Comment effacer un fichier supprimé**

4.0 Avant de commencer

Dans cette section, nous verrons comment récupérer des fichiers préalablement supprimés et comment effacer (ou écraser) des données privées ou sensibles.

Recuva vous permet de créer un nouveau dossier pour y sauvegarder vos fichiers et documents récupérés. Même si **Recuva** vous laisse choisir un dossier pré-existant, pour des raisons de sécurité, il est recommandé de sauvegarder vos fichiers récupérés sur un support amovible, comme un disque dur externe ou une clé USB.

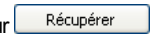
Important: Bien que **Recuva** soit très efficace pour écraser des données, il est possible que le programme laisse derrière lui des identifiants de fichiers qui peuvent révéler l'existence de ces fichiers. Pour protéger votre sécurité et votre confidentialité, il est plus logique de sauvegarder toutes vos données importantes, privées ou sensibles sur des dispositifs amovibles plutôt qu'à l'emplacement original des fichiers.

4.1 Comment récupérer un fichier supprimé

Pour récupérer un fichier supprimé, suivez les étapes énumérées ci-dessous:

Première étape. **Connectez** un disque dur externe ou une clé USB à votre ordinateur.

Deuxième étape. **Cochez** la case à cocher qui correspond au fichier que vous souhaitez récupérer pour activer le bouton *Récupérer...* ou **double cliquez** ce fichier pour cocher *et* surligner ce fichier simultanément.

Troisième étape. **Cliquez** sur 

pour afficher la fenêtre *Rechercher un dossier*.

Quatrième étape. **Sélectionnez** une destination puis **cliquez** sur Créer un nouveau dossier afin de créer un dossier pour vos fichiers récupérés, tel qu'illustré à la *Figure 1* ci-dessous.

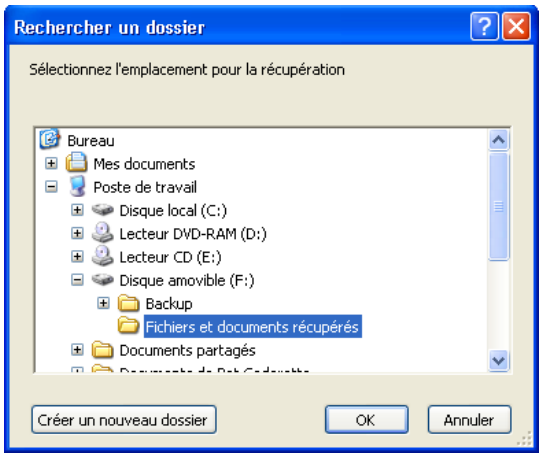


Figure 1: La fenêtre Rechercher un dossier affichant le nouveau dossier créé sur un disque du dur externe

Commentaire: Dans cet exemple, le nouveau dossier s'est vu donner un nom explicite. Cependant, toujours dans l'optique de préserver votre confidentialité et votre sécurité numérique, nous vous encourageons à donner un nom plus discret au dossier que vous créerez pour y sauvegarder vos données privées et sensibles.

Cinquième étape. **Cliquez** sur Yes pour lancer le processus de récupération de vos fichiers supprimés; vous verrez apparaître une fenêtre affichant une barre de progression, tel qu'illustré ci-dessous:

Figure 2: La barre de progression du processus de récupération des fichiers

Lorsque les fichiers seront récupérés, une fenêtre de confirmation s'affichera:

Figure 3: La fenêtre Opération terminée

Commentaire: **Recuva** peut récupérer plusieurs fichiers en une seule opération. Vous n'avez qu'à cocher tous les fichiers que vous souhaitez récupérer et suivre les consignes des **étapes 4 à 5**.

Maintenant que vous savez comment récupérer des fichiers supprimés, nous verrons maintenant comment utiliser le menu contextuel pour exécuter une récupération de plusieurs fichiers et/ou écraser des fichiers.

4.2 Comment utiliser le menu contextuel

Recuva offre différentes options pour sélectionner des documents, fichiers ou dossiers que vous souhaiteriez récupérer ou écraser.

- **Cocher**: Habituellement, on coche pour sélectionner rapidement plusieurs fichiers non contigus ou séparés afin de les récupérer ou les écraser.
- **Surligner**: Habituellement, on surligne pour sélectionner rapidement plusieurs fichiers contigus en bloc ou en groupe afin de les récupérer ou les écraser.

Cliquez à droite sur un fichier supprimé affiché dans l'interface principale de **Recuva** pour afficher le menu contextuel suivant:

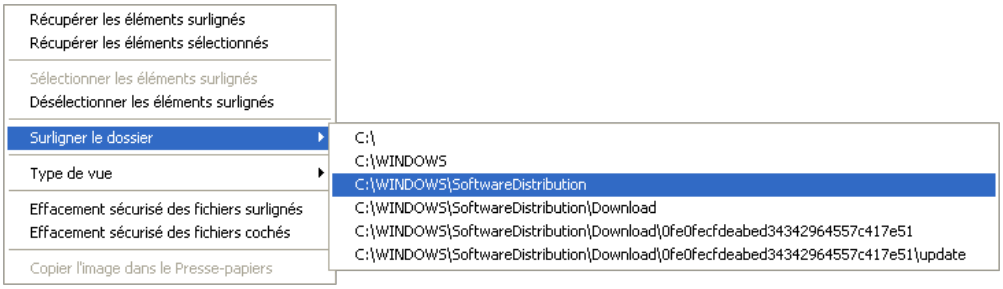


Figure 4: Le menu contextuel

Récupérer les éléments surlignés: Cette option vous permet de récupérer tous les fichiers que vous avez surlignés.

Récupérer les éléments sélectionnés: Cette option vous permet de récupérer un fichier dont vous avez coché la case à cocher.

Sélectionner les éléments surlignés: Cette option vous permet de cocher le(s) fichier(s) surligné(s).

Dessélectionnez les éléments surlignés: Cette option vous permet de décocher les fichiers surlignés.

Comme nous l'avons vu, le **Type de vue** peut également être défini dans l'onglet *Général* de la fenêtre *Options*. Cette option-ci vous permet de définir les fichiers supprimés s'afficheront.

- **Liste**: Cette option vous permet d'afficher les fichiers supprimés sous forme de liste, tel qu'illustré à la *Figure 5*.
- **Arborescence**: Cette option vous permet d'afficher l'emplacement des fichiers supprimés sous forme d'arborescence extensible.
- **Vignettes**: Cette option vous permet d'afficher les fichiers supprimés sous forme de graphiques ou d'images lorsque cela est possible.

Surligner le dossier: Cette option vous permet de sélectionner plusieurs fichiers supprimés en fonction de leur chemin d'accès au répertoire, et d'exécuter sur eux les actions listées dans le menu contextuel.

Effacement sécurisé des fichiers surlignés: Cette option vous permet d'effacer le fichier supprimé surligné.

Effacement sécurisé des fichiers cochés: Cette option vous permet d'effacer un fichier supprimé, ce qui change son icone d'état du vert au rouge.

4.3 Comment écraser un fichier supprimé

Pour écraser/effacer un fichier supprimé, suivez les étapes énumérées ci-dessous:

Première étape. **Cochez** le fichier que vous voulez écraser/effacer, puis **cliquez à droite** sur la case à cocher pour afficher le menu contextuel.

Deuxième étape. **Sélectionnez** Effacement sécurisé des fichiers cochés pour afficher la boîte de dialogue de confirmation suivante:

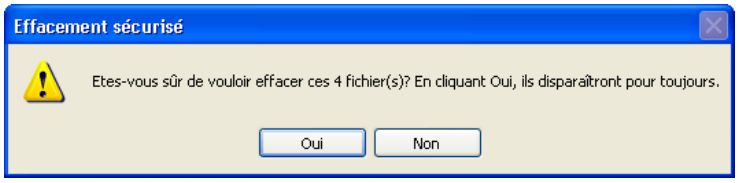

Effacement sécurisé
Etes-vous sûr de vouloir effacer ces 4 fichier(s)? En cliquant Oui, ils disparaîtront pour toujours.
Oui
Non

Figure 5: La boîte de dialogue de confirmation Effacement sécurisé

Troisième étape. **Cliquez** sur Yes pour lancer le processus d'effacement; selon la taille et l'état du fichier, ainsi que le paramètre de l'*Effacement sécurisé* que vous avez défini dans l'onglet *Général* de la fenêtre *Options*, cette opération peut prendre un certain temps. Lorsque le processus d'effacement est complété, une fenêtre comme celle-ci s'affiche:

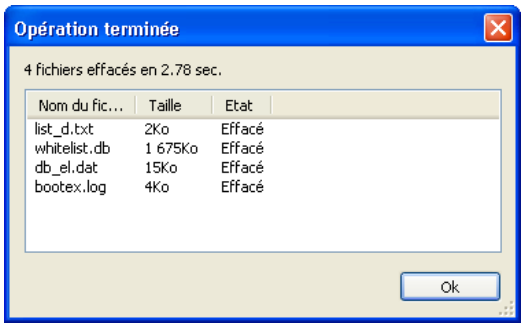


Figure 6: La fenêtre Opération terminée

Vous avez réussi à utiliser **Recuva** pour récupérer et effacer des fichiers préalablement supprimés. Pour réviser votre connaissance du programme **Recuva** veuillez consulter la section **FAQ et questions récapitulatives** [103]

Faq et questions récapitulatives

Elena et Nikolai sont enchantés par les possibilités que leur offre **Recuva**, et surtout par la facilité d'utilisation et l'efficacité du programme. Ils sont maintenant curieux de connaître ses options avancées et ont quelques questions supplémentaires.

***Q**: Y a-t-il des types de fichiers que **Recuva** ne peut pas récupérer?*

***A**: Non, **Recuva** peut récupérer n'importe quel type de fichiers.*

***Q**: Est-ce que je peux récupérer un fichier qui a été écrasé/effacé de façon sécurisée?*

***A**: Une fois qu'un fichier a été effacé de façon sécurisée, il est disparu pour toujours.*

***Q**: J'ai remarqué que parfois, même après qu'un fichier ait été effacé, il reste identifié comme récupérable. Comment est-ce possible?*

***A**: Il est possible que ce que tu vois est un identifiant de fichier, une balise indiquant l'emplacement original du fichier. Par contre, si tu récupères et que tu ouvres ce fichier, tu verras que son contenu est illisible.*

***Q**: J'ai supprimé un fichier par accident; comme je l'avais créé à peine cinq minutes auparavant, je croyais qu'il allait être assez facile de le récupérer. Comment se fait-il que **Recuva** soit incapable de le récupérer?*

A: Ironiquement, un document ou un fichier qui n'existe que depuis quelques minutes est plus susceptible d'être écrasé par des fichiers temporaires qu'un fichier qui existe depuis plus longtemps. **Recuva** ne récupère pas

facilement des fichiers qui ont été supprimés peu après leur création.*

***Q**: Suite à un nettoyage de mon système à l'aide de **CCleaner**, est-ce que mes données pourraient être récupérées?*

A: Selon les ressources et les aptitudes de la personne qui tenterait une telle récupération, c'est effectivement possible. Cela dépend aussi des paramètres de l'effacement sécurisé qui ont été définis pour nettoyer les fichiers

temporaires et le **Registre de Windows** avec **CCleaner**. Pour réduire au maximum la possibilité de récupérer des données privées ou sensibles, il est conseillé d'activer l'option Effacement sécurisé dans **CCleaner**, puis d'effacer

l'espace libre du disque dur et du **Windows Master File Table**. Dans **Recuva**, il est possible d'augmenter le nombre de passages utilisés pour écraser des données. C'est une bonne question parce qu'on peut voir comment différents outils peuvent être combinés pour protéger ta confidentialité et ta

sécurité numérique.*

5.1 Questions récapitulatives

- Est-ce que le fait de fermer votre ordinateur réduit la capacité de **Recuva** à récupérer efficacement vos documents, fichiers et dossiers supprimés?
- En quoi le fait d'augmenter le nombre de passages à un effet sur l'effacement sécurisé d'un document ou d'un fichier donné?
- Nommez deux conditions qui ont un effet sur votre capacité à récupérer un document un fichier supprimé dans **recuva**.
- Il y a deux façons d'activer l'*Analyse approfondie* dans **recuva**; quelles sont-elles?
- Dans quelle circonstance est-il indiqué d'utiliser l'*Assistant de Recuva* pour lancer un scan et tenter de récupérer des fichiers supprimés?

Eraser - suppression de fichiers sécurisée

Eraser permet de nettoyer votre ordinateur en supprimant définitivement les fichiers sensibles qui s'y trouvent. Il peut également être utilisé pour nettoyer des dispositifs de stockage amovibles.

Site Internet

www.heidi.ie [104]

Configuration requise :

- Windows 95, 98, ME, NT 4.0, 2000, XP & Vista

Version utilisée pour rédiger ce guide :

- 5.86

Licence :

- FLOSS (Free/Libre and Open Source Software)

Pour installer Eraser

- *Lisez la courte introduction des Guides pratiques [13]*
- ***Cliquez sur l'icône ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

Eraser:

[105]

Lecture préalable :

- Livret pratique Security in-a-box, chapitre 6. Détruire définitivement des données sensibles [106].

Niveau : 1 : Débutant, **2 : Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5: Avancé

Temps d'apprentissage : 20 minutes

Ce que vous apportera l'utilisation de cet outil : :

- La capacité de supprimer définitivement de votre ordinateur des fichiers de nature « délicate ».
- La capacité de supprimer définitivement de votre ordinateur tous les fichiers récupérables qui sont actuellement invisibles.

1.1 À propos de cet outil

Eraser permet de nettoyer votre ordinateur en supprimant définitivement les fichiers sensibles qui s'y trouvent. Pour ce faire, il réécrit par dessus, ou « écrase », les données à effacer. Cette méthode permet de supprimer définitivement aussi bien des fichiers que des répertoires. De plus, Eraser effacera les copies de fichiers qui se trouvent sur votre ordinateur et dont vous ne soupçonnez peut-être même pas l'existence. Cela comprend les fichiers que vous avez déjà supprimés par l'interface de **Windows**, ainsi que les copies des documents sur lesquels vous avez travaillé dans le passé.

1. Eraser permet d'effacer les fichiers ponctuellement ou à intervalle régulier.
2. Si vous choisissez de le faire à intervalle régulier, il faut absolument que l'ordinateur soit allumé au moment prévu, sinon la suppression des fichiers ne sera pas effectuée.
3. Une fois qu'un fichier est supprimé par Eraser, il est impossible de le récupérer à l'aide d'un outil de récupération de données.
4. Pour plus de sécurité, il est recommandé d'écraser les fichiers entre trois et sept fois.
5. Eraser permet également de supprimer/réécrire tout l'espace libre restant sur votre ordinateur. Cela signifie qu'il peut supprimer toutes les traces de vos travaux passés (potentiellement récupérables parce qu'ils n'ont pas été supprimés définitivement).

Comment régler les options d'Eraser

Tel que décrit au chapitre 6. Détruire définitivement des données sensibles [106] du livret pratique, **Eraser** supprime les données sur le disque en les écrasant avec d'autres données aléatoires. Plus le nombre de réécritures est élevé (pour écraser les fichiers), plus il sera difficile de les récupérer.

Commentaire : Nous recommandons d'écraser les données au moins trois fois.

Conseil : Notez que chaque « passe » de réécriture prend un certain temps et que plus le nombre de passes est élevé, plus long sera le processus de suppression du fichier. Évidemment, cet effet sera davantage ressenti lors de la suppression de fichiers volumineux ou lors de la suppression/réécriture de l'espace libre.

Le nombre de passes peut être choisi en accédant au menu *Preferences: Erasing*.

Première étape. **Sélectionnez**: **Edit > Preferences > Erasing**, comme suit :

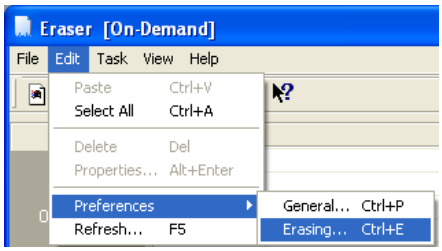


Figure 1 : La fenêtre Eraser [On-demand] affichant les options du menu Edit

La fenêtre Preferences:Erasing *s'affiche comme suit* :

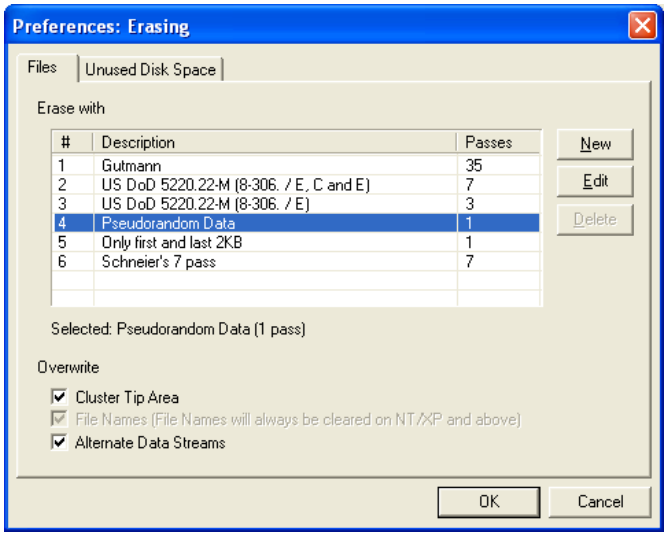


Figure 2 : La fenêtre Preferences: Erasing

La fenêtre *Preferences: Erasing* décrit la méthode utilisée pour la suppression/réécriture des fichiers.

Description: Les noms des procédures de réécriture sont affichés dans cette colonne.
Passes: Le nombre de passes de réécritures utilisées pour chaque méthode.

Nous allons écraser nos données en utilisant la méthode *Pseudorandom Data*. Par défaut, cette méthode comprend une seule passe de réécriture. Par souci de sécurité, nous allons augmenter cette valeur à 3.

Deuxième étape. **Sélectionnez** : *# 4 Pseudorandom Data*, tel qu'illustré à la *figure 2*.

Troisième étape. **Cliquez** sur *Edit* pour faire apparaître la fenêtre *Passes*, illustrée ci-dessous :

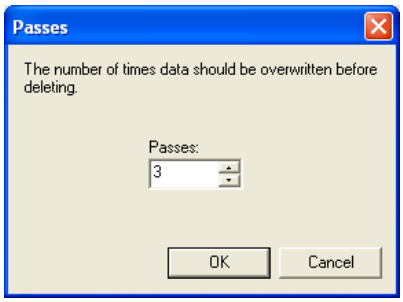


Figure 3 : La fenêtre Passes d'Eraser

Quatrième étape. Choisissez un nombre de passes entre 3 et 7 (tenez compte autant du temps requis pour chaque passe que du niveau de sécurité souhaité).

Cinquième étape. **Cliquez** sur le bouton *OK* pour revenir à la fenêtre *Eraser Preferences: Erasing*.

L'option # 4 Pseudorandom Data *devrait maintenant ressembler à ceci :*

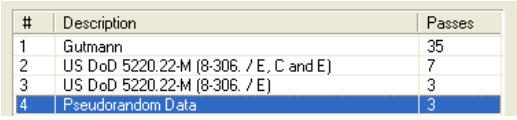


Figure 4 : La fenêtre Preferences: Erasing *avec l'option 4 sélectionnée.*

Conseil : Assurez-vous que les options *Cluster Tip Area* et *Alternate Data Streams* sont sélectionnées (elles devraient l'être par défaut).

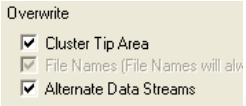


Figure 5 : Les options Cluster Tip Area et Alternate Data Streams sélectionnées par défaut.

- *Cluster Tip Area* : Un disque dur est divisé en plusieurs segments que l'on nomme *clusters* ou « blocs ». Habituellement, un fichier est contenu sur plusieurs blocs, sans toutefois remplir complètement le dernier bloc qu'il occupe. La partie vacante à la fin du dernier bloc se nomme la *Cluster Tip Area* ou « Zone de fin de bloc ». Cette Zone de fin de bloc peut contenir une partie des données sensibles d'un autre fichier ayant précédemment occupé cet espace du bloc. Les données qui se trouvent dans cette zone peuvent être récupérées par un spécialiste. Assurez-vous donc de **cocher** cette case!
- *Alternate Data Streams* : Un fichier stocké sur un ordinateur peut comporter plusieurs parties. Par exemple, le présent document contient du texte et des images. Ces différents éléments sont stockés à différents emplacements du disque : c'est ce que sont les *streams* ou « trames de données ». **Cocher** cette option vous assure que toutes les « Trames de données alternatives » associées aux fichiers seront effacées.

Sixième étape. **Cliquez** sur le bouton *OK*.

Vous venez de configurer la méthode utilisée pour écraser les fichiers dans Eraser. Vous devriez choisir les mêmes options dans l'onglet suivant de la fenêtre *Preferences : Erasing*, c.-à-d. l'onglet *Unused Disk Space*. Cela dit, tenant en considération que chaque passe prendra environ deux heures, vous pouvez y spécifier un nombre de passes moins élevé.

Comment utiliser Eraser

3.1 Comment utiliser Eraser avec Windows Explorer

L'application la plus fréquente d'**Eraser** ne passe pas par le programme lui-même, mais plutôt par la fenêtre du *Poste de travail* de l'**Explorateur Windows**.

Première étape. **Ouvrez** un dossier où se trouve un fichier que vous souhaitez supprimer définitivement.

Deuxième étape. **Cliquez à droite** sur le fichier voulu. Deux nouvelles options s'offrent maintenant à vous dans le menu défilant, c.-à-d. *Erase* et *Eraser Secure Move*.

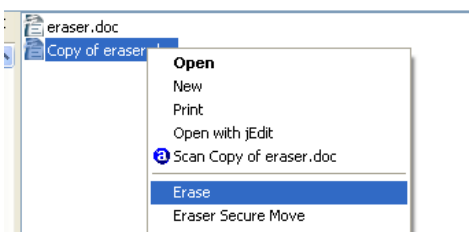


Figure 6. Les options Erase et Eraser Secure Move

Nous utiliserons l'option *Erase* pour supprimer ce fichier définitivement.

Troisième étape. **Sélectionnez** : **Erase** dans le menu.

Vous verrez alors apparaître la boîte de dialogue Confirm Erasing*, illustrée ci-dessous :*

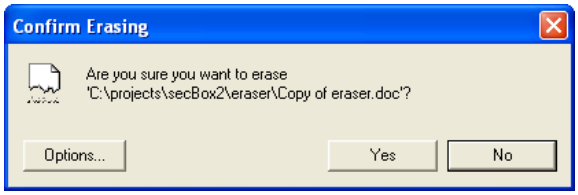


Figure 7 : La boîte de dialogue Confirm Erasing

Si le fichier décrit correspond bien à celui que vous souhaitez supprimer définitivement, passez à l'étape suivante :

Quatrième étape. **Cliquez** sur le bouton *Yes*.

Le fichier sera alors supprimé définitivement du système.

Avertissement : Lorsque vous effacez un fichier de cette façon, il est perdu à jamais. Vous ne pourrez PAS le récupérer. Assurez vous de n'effacer que les fichiers que vous ne voulez pas conserver sur votre ordinateur.

Pour transférer un ou plusieurs fichiers de façon sécurisée d'un emplacement à un autre (par exemple de votre ordinateur à une clé USB) :

Cinquième étape. **Sélectionnez** : **Eraser Secure Move**.

Vous devrez répondre au même message d'avertissement que précédemment pour continuer.

3.2 Comment « nettoyer » l'espace libre du disque dur

Le nettoyage, ou la réécriture, de l'espace inutilisé du disque dur implique la suppression définitive de toutes les traces des fichiers qui se trouvaient préalablement dans « l'espace libre » de votre disque dur ou de votre dispositif de stockage amovible. Cet espace vide peut contenir des fichiers qui n'ont pas été intégralement supprimés. (À ce sujet, voir le guide pratique Undelete Plus [107] et le chapitre 6 [108] du livret pratique Security in-a-box.)

Première étape. **Sélectionnez** : **Démarrer > Programmes > Eraser > Eraser**

Conseil : Vous pouvez soit lancer une tâche ponctuelle de nettoyage de l'espace libre, soit planifier une tâche automatique à intervalle régulier.

Important : Ce processus peut prendre de 2 à 5 heures et ralentira votre ordinateur si vous l'utilisez en même temps. Il est donc conseillé de planifier une tâche de nettoyage de l'espace libre à un moment qui n'entre pas en conflit avec votre utilisation de l'ordinateur (par exemple, la nuit, quand vous ne travaillez pas).

3.3 Comment utiliser l'option de réécriture ponctuelle (*On-Demand*)

Pour créer une tâche de réécriture ponctuelle (*On-Demand*) pour effacer l'espace inutilisé du disque dur, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur :

Deuxième étape. **Sélectionnez** : **File > New Task**, comme suit :

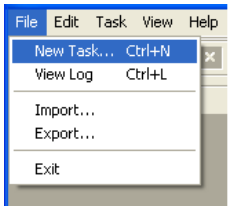


Figure 8 : Ouvrir une nouvelle tâche dans le menu File

L'option *Unused space on drive* devrait déjà être cochée.

Troisième étape. **Sélectionnez** le disque dont l'espace libre doit être nettoyé. (Dans l'exemple ci-dessous, le *disque local (C :)* est sélectionné. Il s'agit habituellement du disque principal sur la plupart des ordinateurs.)

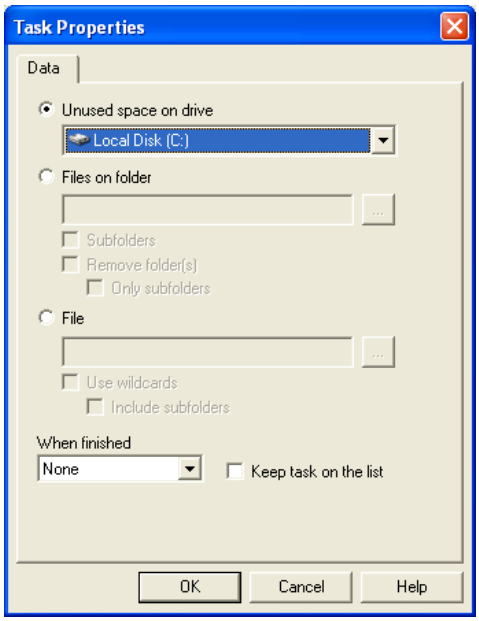


Figure 9 : La fenêtre Task Properties d'Eraser

Quatrième étape. **Cliquez** sur le bouton *OK*.

La tâche est maintenant créée et devrait être lancée automatiquement. La nouvelle tâche devrait être affichée dans la fenêtre principale d'Eraser.

Cinquième étape. **Cliquez à droite** sur la tâche pour activer le menu défilant illustré ci-dessous :

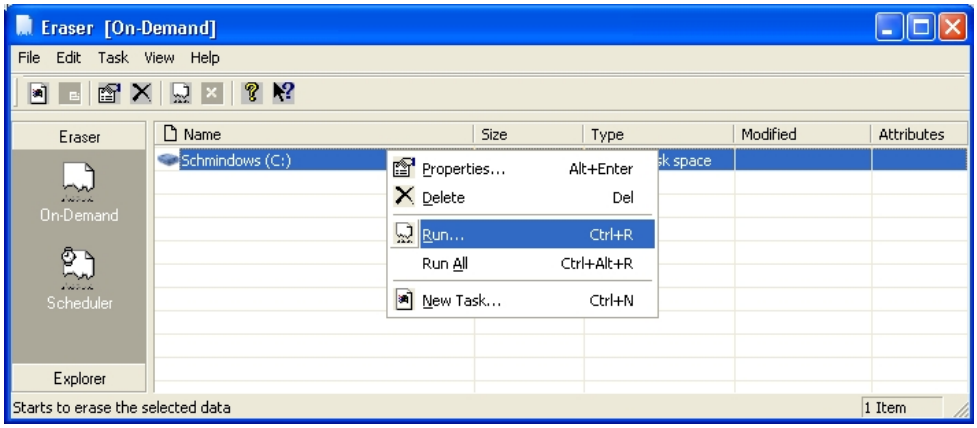


Figure 10 : La fenêtre principale d'Eraser avec l'option Run *sélectionnée*

Sixième étape. **Sélectionnez** : **Run** pour activer la boîte de dialogue suivante :

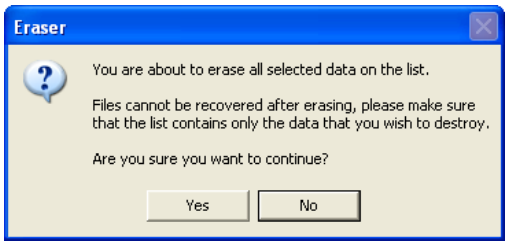

Eraser
You are about to erase all selected data on the list.
Files cannot be recovered after erasing, please make sure that the list contains only the data that you wish to destroy.
Are you sure you want to continue?
Yes
No

Figure 11. La boîte de dialogue Eraser

Septième étape. **Cliquez** sur le bouton *Yes*.

Une barre de progrès apparaît, et Eraser procède au nettoyage de l'espace vide.

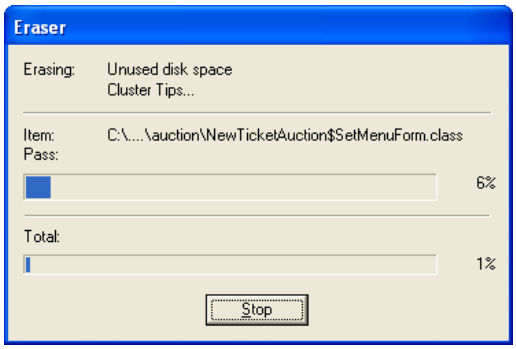


Figure 12 : La fenêtre d'Eraser

3.4 Comment utiliser l'option de nettoyage par tâche planifiée

Comme il est souvent trop facile d'oublier d'entretenir son ordinateur convenablement, **Eraser** offre la possibilité de lancer automatiquement les tâches de nettoyage à intervalle quotidien ou hebdomadaire, à une heure définie d'avance.

Première étape. **Cliquez** sur :

dans la fenêtre principale d'Eraser.

Deuxième étape. **Sélectionnez** : **File > New Task**, comme suit :

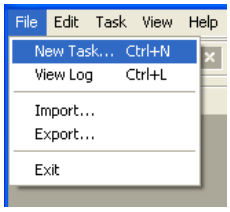


Figure 13 : Ouvrir une nouvelle tâche dans le menu File

La fenêtre qui s'affiche alors ressemble à celle qui nous a permis de définir une tâche ponctuelle.

Troisième étape. **Réglez** ces options comme précédemment, à la section **3.3 Comment utiliser l'option de suppression/réécriture ponctuelle**.

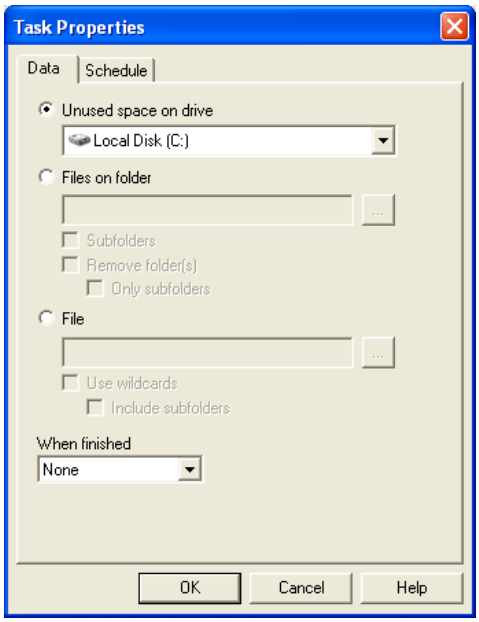


Figure 14 : La fenêtre Task Properties d'Eraser affichant l'onglet Schedule

Quatrième étape. **Cliquez** sur l'onglet *Schedule*.

L'onglet *Schedule* affiche les options suivantes :

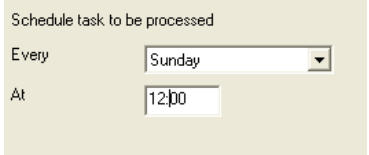


Figure 15 : L'onglet Schedule d'Eraser

Commentaire : En cliquant sur le menu déroulant *Every*, vous aurez le choix de lancer la tâche à intervalle quotidien ou hebdomadaire. La deuxième option permet de choisir l'heure à laquelle vous souhaitez lancer la tâche.

Cinquième étape. Après avoir défini l'intervalle de la tâche, **cliquez** sur le bouton *OK*.

La tâche planifiée s'affichera comme ceci :

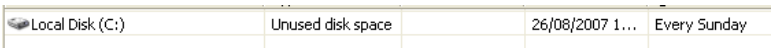


Figure 16 : La liste des tâches planifiées d'Eraser

Commentaire : Pour que la tâche planifiée soit exécutée, il est nécessaire que l'ordinateur soit en fonction à l'heure choisie pour la tâche.

3.5 Comment éliminer une tâche

Après avoir lancé ou planifié une tâche, vous voudrez peut-être l'enlever de votre liste de tâches.

Pour éliminer une tâche ponctuelle, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur :

pour afficher la liste des tâches, tel qu'illustré ci-dessous :

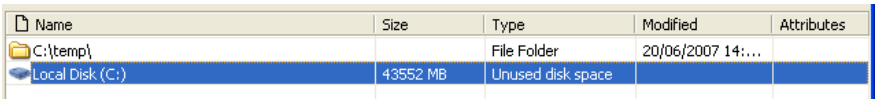


Figure 17 : La liste des tâches d'Eraser

Deuxième étape. **Sélectionnez** la tâche que vous souhaitez éliminer (la tâche sélectionnée sera surlignée en bleu, tel qu'illustré dans la figure 17).

Troisième étape. **Cliquez** sur :

La tâche sera alors retirée de la liste.

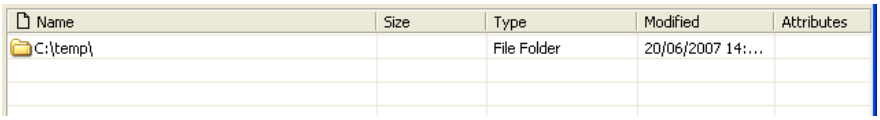


Figure 18 : La liste des tâches d'Eraser, avec la tâche ponctuelle en moins

La procédure pour éliminer une tâche planifiée est pratiquement identique. Pour ce faire, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur :

Répétez les étapes 2 et 3 énumérées ci-dessus pour éliminer une tâche ponctuelle.

Faq et questions récapitulatives

Elena et Nikolai trouvent **Eraser** assez facile à utiliser, mais ils se rendent bien compte que c'est un programme qui doit être manipulé avec précaution, puisque les éléments qui sont supprimés de cette façon seront irrécupérables. Ils ont l'impression qu'il est important de prendre le temps d'apprendre à bien connaître le programme avant de s'en servir régulièrement. Eraser semble bien fonctionner sur l'ordinateur d'Elena, mais ils ont encore quelques questions à propos d'Eraser.

Q. : *Puis-je utiliser Eraser pour supprimer des fichiers qui se trouvent sur ma clé USB?*

R. : *Oui. Tu peux supprimer ces fichiers définitivement par l'interface **Explorateur Windows**. Tu peux également effacer/réécrire l'espace libre sur ta clé USB en créant une tâche appropriée dans Eraser.*

Q. : *Si je ne veux plus utiliser Eraser, est-ce qu'il est facile de désinstaller le programme? Et si je le désinstalle, est-ce que cela aura un effet sur mon ordinateur? Et mes fichiers demeureront-ils supprimés?*

R. : *Tu peux désinstaller Eraser à partir du menu Démarrer. Sélectionne **Démarrer > Programmes > Eraser > Uninstall Eraser**. Cela n'affectera en rien les autres programmes installés sur ton ordinateur, et les fichiers que tu as déjà supprimés ne seront pas récupérables.*

Q. : *Y a-t-il des fichiers **Windows** qu'Eraser ne supprime pas?*

R. : *Tous les fichiers qui se trouvent sur ton ordinateur peuvent être supprimés définitivement par Eraser. Même certains fichiers invisibles (tel que les fichiers récupérables se trouvant dans l'espace libre) seront supprimés définitivement si tu configures adéquatement les options que nous avons vues.*

Q. : *Est-ce qu'Eraser supprime aussi les noms des fichiers?*

R. : *Oui, toutes les parties du fichier sont supprimées définitivement. Cependant, tu devrais utiliser CCleaner [108] pour supprimer la liste des documents récents.*

Q. : *Est-ce qu'il sera possible à quelqu'un d'accéder aux fichiers supprimés?*

R. : *La récupération des données de fichiers qui ont été écrasés est un processus extrêmement complexe et onéreux. Le temps requis pour restaurer un fichier qui n'a été écrasé qu'une seule fois est démesuré, alors imagine le temps qu'il faut pour restaurer un fichier écrasé de trois à sept fois! Si tu utilises Eraser de façon adéquate, tu peux être certain que tes données ont été supprimées définitivement.*

4.1 Questions récapitulatives

1. Quel genre d'information Eraser peut-il effacer de votre ordinateur?
2. Qu'entend-on par « espace libre / inutilisé »?
3. Comment Eraser supprime-t-il vos données?
4. Quel est le nombre de passes minimum recommandé avec Eraser?
5. Comment configure-t-on le nombre de passes minimum dans Eraser?
6. Comment planifie-t-on une tâche automatique dans Eraser?
7. Comment peut-on effacer un répertoire qui se trouve dans un autre répertoire?
8. Comment peut-on effacer plusieurs fichiers à la fois?

CCleaner - suppression de fichiers et nettoyage sécurisés

Short Description:

CCleaner est un programme efficace et facile à utiliser pour protéger votre sécurité et votre confidentialité numérique. En supprimant de façon permanente votre historique de navigation, vos cookies et autres fichiers temporaires générés automatiquement lors de vos séances de travail, et en nettoyant l'espace libre de vos disque durs, **CCleaner** limite les moyens par lesquels des tiers partis hostiles ou malveillants pourraient contrôler vos préférences et habitudes de travail ou infecter votre système.

Online Installation Instructions:

Pour installer CCleaner

- *Lisez la courte **Introduction** aux **Guides pratiques** [1]*
- ***Cliquez** sur l'icone **CCleaner** ci-dessous pour ouvrir la page de téléchargement **www.piriform.com/ccleaner/builds***
- *Dans la section 'CCleaner - Slim' **cliquez** sur le bouton de 'téléchargement'*
- ***Sauvegardez** l'exécutable 'ccsetup_slim.exe' sur votre ordinateur, puis **double-cliquez** sur l'icone pour lancer l'installation du programme*
- *Lisez attentivement les 'consignes d'installation' détaillées à la prochaine section avant de continuer*
- *Après avoir complété l'installation de **CCleaner** vous pouvez supprimer l'exécutable d'installation de votre ordinateur*

CCleaner:

[109]

Site Internet

www.ccleaner.com [110]

Configuration requise

- Compatible avec toutes les versions de Windows

Version utilisée pour rédiger ce guide

- 2.33

Licence

- Gratuiciel

Lecture préalable

Livret pratique Security-in-a-Box, chapitre 6. Détruire définitivement des données sensibles [37]

Niveau: 1: Débutant, **2: Moyen**, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 15 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de supprimer définitivement toutes traces de vos activités et des fichiers temporaires stockés sur votre ordinateur.
- La capacité de **nettoyer l'espace libre des disques** connectés à votre ordinateur
- La capacité de nettoyer le **Registre de Windows**
- La capacité de **déterminer quels programmes sont activés au démarrage de votre ordinateur**

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

BleachBit [111] est un autre excellent outil de suppression et de destruction de fichiers temporaires, compatible avec **GNU Linux** et **Microsoft Windows**. **BleachBit** vous permet de supprimer les fichiers temporaires générés par 70 des applications les plus répandues et par le système d'exploitation, et de libérer de l'espace sur vos disques durs. Un programme de code

source libre proposant une version portable, **BleachBit** est disponible en 32 langues. Les utilisateurs de **Ubuntu Linux** peuvent en outre se référer au guide Nettoyer Ubuntu… [112] pour apprendre à nettoyer leur système.

Les utilisateurs de **Mac OS** apprécieront sûrement les outils gratuits proposés par Titanium's Software: **OnyX** et **Maintenance** [113] pour supprimer les traces de vos séances de travail. Pour effacer de façon sécuritaire le contenu de votre *Trash*, ouvrez l'application *Finder* et sélectionnez le menu *Finder* > *Secure Empty Trash*. Vous pouvez choisir de toujours supprimer le contenu de votre *Trash* de façon sécuritaire en ouvrant les préférences *Avancées* du Finder et en cochant l'option *Empty Trash securely*. Pour nettoyer l'espace libre de votre disque dur, lancez l'application système *Disk Utility*, sélectionnez la partition voulue, sélectionnez l'onglet *Erase* et cliquez sur le bouton *Erase Free Space.*

1.1 À propos de cet outil

Les paramètres par défaut de votre système et de votre navigateur Web génèrent automatiquement une trace de vos données dont un tiers parti hostile ou malveillant pourrait tirer avantage, un peu comme un chasseur traquant sa proie. Chaque fois que vous utilisez un navigateur ou un logiciel de traitement de texte, ou tout autre programme, des fichiers et données temporaires sont générés et stockés quelque part sur votre ordinateur. Ces programme génèrent également des listes de documents ou pages Internet récemment consultés. Par exemple, chaque fois que vous saisissez une adresse Internet dans votre navigateur préféré, une liste des adresses qui commencent avec les mêmes caractères s'affichent automatiquement, comme ceci:

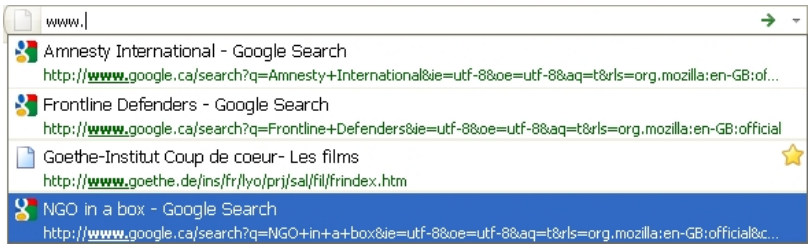


Figure 1: Une barre d'adresse de navigateur affichant différentes URLs

Bien que les historiques des navigateurs puissent êtres utiles à l'occasion, elle peuvent aussi permettre à un tiers parti d'identifier les sites Internet que vous avez visités. De plus, vos activités récentes peuvent être exposées par les données temporaires sauvegardées à partir des images comprises dans ces sites Internet., y compris les messages de courrier électronique et les coordonnées saisies dans des formulaires.

Pour supprimer les données temporaires générées chaque fois que vous utilisez un programme, il vous faudrait ouvrir chaque répertoire de chaque programme, identifier et supprimer manuellement chaque fichier temporaire. **CCleaner affiche une liste de programmes et vous laisse choisir le ou les programme(s) dont vous souhaitez supprimer les fichiers temporaires.

Important: Même si **CCleaner** ne supprime que les fichiers temporaires, et non pas les documents sauvegardés sur votre ordinateur, il est **fortement recommandé** que vous conserviez une sauvegarde mise à jour de vos documents (veuillez consulter le **Livret pratique** Security-in-a-Box, chapitre **5. Récupérer des données perdues** [94] pour plus de conseils sur la création de copies de sauvegarde).

Après avoir lancé **CCleaner**, il est possible que vous ayez perdu les historiques de votre navigateur et de vos documents récents, ainsi que vos mots de passe sauvegardés. C'est précisément la fonction de cet outil, c'est-à-dire de minimiser les différentes façons par lesquelles des tiers partis malveillants pourraient infecter ou espionner votre système.

Comment installer et configurer CCleaner

Sommaire des sections de cette page:

- **2.0 Comment installer CCleaner**
- **2.1 Avant de commencer à configurer CCleaner**

2.0 Comment installer CCleaner

L'installation de **CCleaner** est relativement simple et rapide. Pour lancer l'installation de **CCleaner**, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** sur ccsetup235_slim pour lancer le processus d'installation. Il est possible que s'ouvre une boîte de dialogue *Fichier ouvert - Avertissement de sécurité*. Si c'est le cas, **cliquez** sur Exécuter pour afficher la fenêtre suivante:

Figure 1: La boîte de sélection de la langue de l'assistant

Deuxième étape. **Cliquez** sur OK pour afficher l'assistant d'installation de CCleaner.

Troisième étape. **Cliquez** sur Suivant > pour afficher la fenêtre de la *licence utilisateur de CCleaner*. Veuillez lire

attentivement la *Licence utilisateur* avant de poursuivre le processus d'installation.

Quatrième étape. **Cliquez** sur J'accepte pour afficher la fenêtre *Choisissez le dossier d'installation*.

Cinquième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Options d'installation*.

Commentaire: Si la fenêtre *Options d'installation* s'affiche avec l'option *Add CCleaner Yahoo! toolbar and use CCleaner from your browser* sélectionnée par défaut, dessélectionnez cette option parce qu'elle pourrait compromettre votre confidentialité sur Internet. (NDT: Dans la version v2.35, cette option a été éliminée du processus d'installation.)

Sixième étape. **Cliquez** sur l'option *Add CCleaner Yahoo! toolbar and use CCleaner from your browser* pour la dessélectionner.

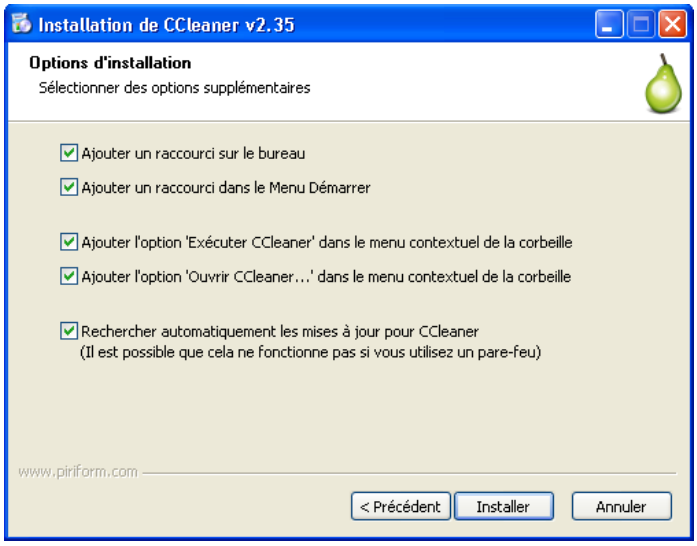

Installation de CCleaner v2.35
Options d'installation
Sélectionner des options supplémentaires
Ajouter un raccourci sur le bureau
Ajouter un raccourci dans le Menu Démarrer
Ajouter l'option 'Exécuter CCleaner' dans le menu contextuel de la corbeille
Ajouter l'option 'Ouvrir CCleaner...' dans le menu contextuel de la corbeille
Rechercher automatiquement les mises à jour pour CCleaner
(Il est possible que cela ne fonctionne pas si vous utilisez un pare-feu)
www.piriform.com
< Précédent
Installer
Annuler

Figure 2: Les options d'installation avec la barre d'outil Yahoo!

Septième étape. **Cliquez** sur Installer pour lancer l'installation de **CCleaner** et afficher la fenêtre *Installation en cours* affichant la barre d'état de l'installation.

Huitième étape. **Cliquez** sur Fermer pour finaliser l'installation de **CCleaner** et activer l'interface utilisateur de *Piriform CCleaner*.

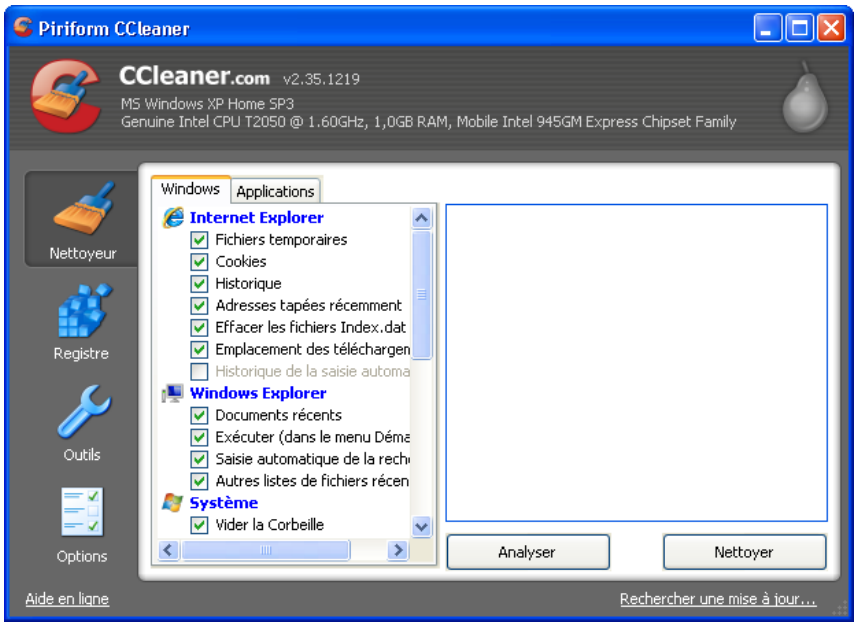


Figure 3: L'interface utilisateur de Piriform CCleaner

2.1 Avant de commencer à configurer CCleaner

Tel que décrit en détail dans le chapitre 6. Détruire définitivement des données sensibles [37] du Livret pratique, les méthodes standard de suppressions de fichiers de **Microsoft Windows** ne suppriment pas réellement les données du disque (et ce, même lorsque vous videz votre corbeille). Même chose pour les fichiers temporaires. Pour supprimer ces fichiers de façon permanente du disque dur (ce qu'on appelle 'nettoyer' ou 'effacer' le disque), il faut écraser les données en question avec des données aléatoires. **CCleaner** doit être configuré pour écraser les fichiers qu'il supprime et ainsi les nettoyer de façon sécuritaire (le programme n'est pas réglé de cette façon par défaut). **CCleaner** peut également supprimer de vieilles données inutiles en nettoyant l'espace libre de votre disque dur (veuillez consulter la section **5.3 Comment nettoyer l'espace disque libre avec CCleaner**).

Avant de commencer à utiliser **CCleaner**, vous devriez le régler pour être en mesure de supprimer les fichiers temporaires de

façon permanente et sécuritaire.

Première étape. **Cliquez** sur ou **sélectionnez Démarrer > Programmes > CCleaner** pour afficher l'interface principale de *Piriform CCleaner*.

Deuxième étape. **Cliquez** sur Options pour afficher la fenêtre suivante:

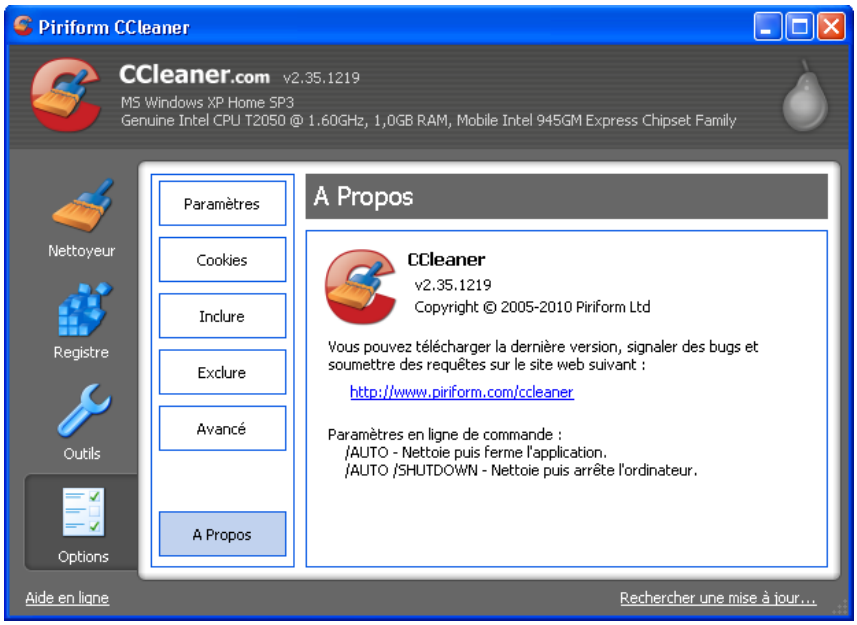


Figure 4: Le panneau à propos

Troisième étape. **Cliquez** sur Paramètres pour afficher le panneau *Paramètres*. Le panneau *Paramètres* vous permet de choisir votre langue de travail et de déterminer comment **CCleaner** supprimera les fichiers temporaires et nettoiera vos disques.

Commentaire: La section *Effacement* s'affiche avec l'option *Effacement normal (Rapide)* sélectionnée par défaut.

Quatrième étape. **Cliquez** sur l'option *Effacement sécurisé (Lent)* pour activer le menu déroulant.

Cinquième étape. **Développez** le menu déroulant et **sélectionnez** l'item *DOD 5220.22 M* de l'option *Effacement sécurisé (Lent)*, tel qu'illustré ci-dessous:

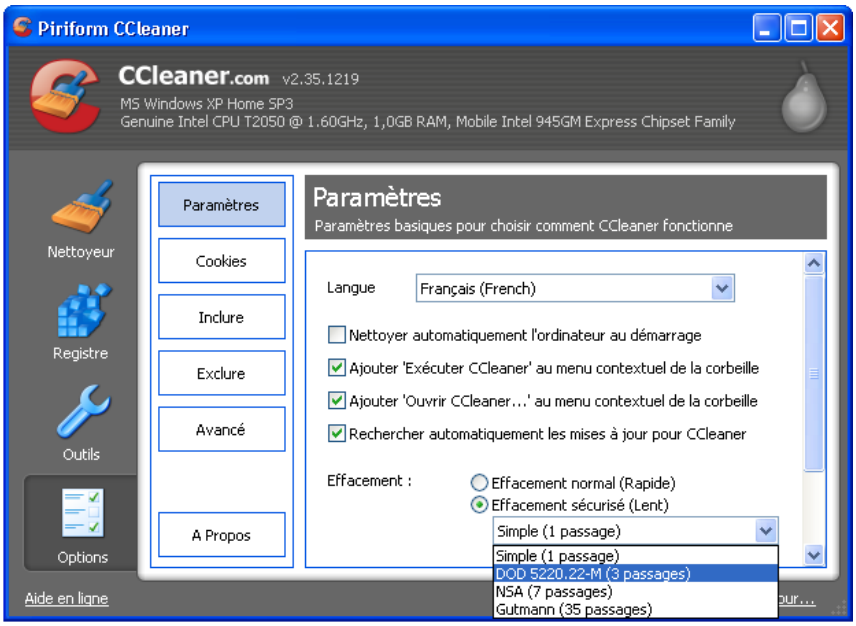


Figure 5: Le panneau Paramètres affichant les options d'Effacement sécurisé

Après avoir configuré cette option, **CCleaner** écrasera les fichiers et dossiers que vous voulez supprimer avec des données aléatoires, ce qui les effacera de façon permanente. Les *Passages* du menu déroulant *Effacement sécurisé* réfère au nombre de fois que les données à effacer seront écrasées par des données aléatoires. Plus le nombre de passages est élevé, plus vos documents, fichiers ou dossiers seront écrasés avec des données aléatoires. Cela réduit considérablement la possibilité de restaurer ces documents, fichiers ou dossiers, mais cela augmente le temps de traitement requis par le processus d'effacement.

Comment supprimer vos fichiers temporaires avec CCleaner

Dans cette section, nous verrons comment supprimer tous les fichiers temporaires générés par **Microsoft Windows** et la plupart des applications que vous utilisez sur votre ordinateur.

Première étape. **Cliquez** sur ou **sélectionnez Démarrer > Programmes > CCleaner** pour afficher la fenêtre principale de **CCleaner**.

Deuxième étape. **Cliquez** sur Nettoyeur pour afficher la fenêtre suivante:

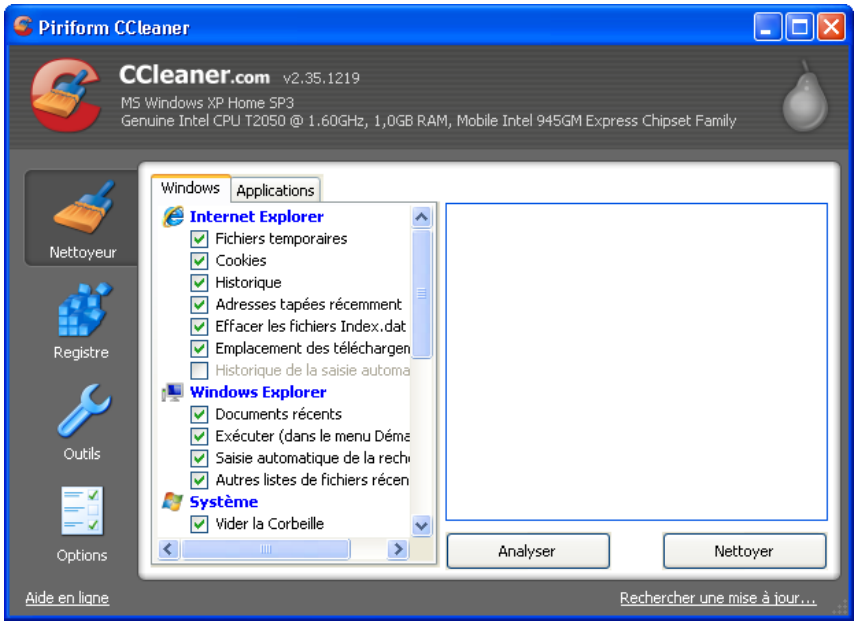


Figure 1: L'interface principale de CCleaner affichant la fenêtre Nettoyeur

La fenêtre *Nettoyeur* est divisée en deux panneaux: le panneau de gauche présente les onglets *Windows* et *Applications*, et le panneau de droite est un espace vide où s'affichent l'information ou les résultats d'une opération de nettoyage donnée. Les boutons * Analyser* et *Nettoyer* se trouve juste en dessous de cet espace.

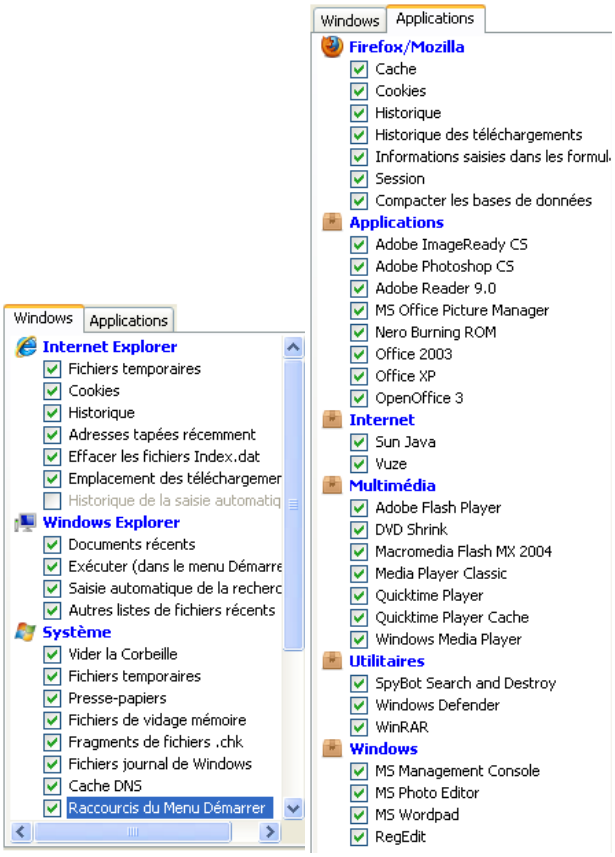


Figure 2: Les onglets Windows et Applications avec toutes les options cochées

Commentaire: En suivant les prochaines étapes, vous supprimerez les fichiers temporaires associés aux items que vous avez cochés dans les onglets *Windows* et *Applications*. Puisque différents utilisateurs ont différents logiciels installés sur leurs ordinateurs, votre propre liste d'applications peut être assez différent de celle que présente la *Figure 2* ci-dessous.

Troisième étape: **Faites défiler** les onglets *Windows* et *Applications* et **cochez** toutes les options de la section *Avancé* également. En cochant certaines options, une boite de dialogue de confirmation s'affiche pour expliquer ce qu'implique chaque option:

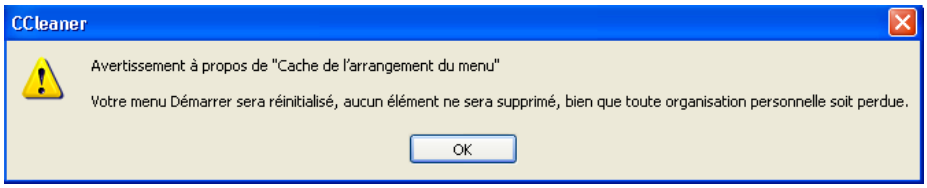

CCleaner
Avertissement à propos de "Cache de l'arrangement du menu"
Votre menu Démarrer sera réinitialisé, aucun élément ne sera supprimé, bien que toute organisation personnelle soit perdue.
OK

Figure 3: Un exemple de boîte de dialogue de confirmation

Commentaire: **Cochez** toutes les options des des onglets *Windows* et *Applications* pour permettre un nettoyage complet et rigoureux des fichiers temporaires. Il est cependant important que vous compreniez bien quels types de réglages et de paramètres sont supprimés.

Quatrième étape. **Cliquez** sur

pour générer une liste de tous les fichiers temporaires pouvant être supprimés.

Astuce: Fermez tous les autres programmes avant d'entamer le processus de nettoyage. Si vous les laissez activés, **CCleaner** ne pourra peut-être pas supprimer tous les fichiers temporaires associés à ces programmes, et il est possible que vous receviez des avertissements comme celui-ci:

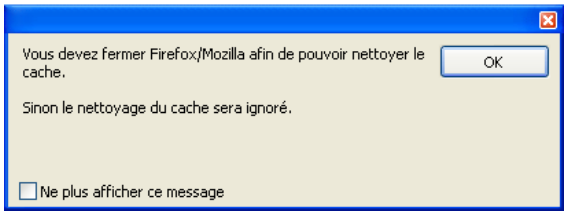
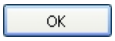

Vous devez fermer Firefox/Mozilla afin de pouvoir nettoyer le cache.
OK
Sinon le nettoyage du cache sera ignoré.
Ne plus afficher ce message

Figure 4: Un exemple de message d'avertissement de fermer Firefox/Mozilla

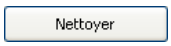
Cinquième étape. **Cliquez** sur 

pour poursuivre l'analyse.

100%
ANALYSE TERMINEE - (148.486 secs)
954,8 Mo à supprimer. (Taille approximative)
Effacement sécurisé des fichiers activé (Simple (1 p
Détails des fichiers à supprimer (Aucun fichier n'a p
Internet Explorer - Fichiers temporaires
Internet Explorer - Cookies
Internet Explorer - Historique
Internet Explorer - Effacer les fichiers Index.d
Windows Explorer - Documents récents
Système - Vider la Corbeille
Système - Fichiers temporaires
Système - Fichiers journal de Windows
Avancé - Vieilles données du Prefetch
Avancé - Désinstalleurs de correctifs Windows
Firefox/Mozilla - Cache
Firefox/Mozilla - Historique des téléchargement
Applications - Office 2003
Applications - Office XP
Analyser
Nettoyer

Figure 5: Un exemple de liste de fichiers temporaires pouvant être supprimés

Commentaire: **CCleaner** supprime les fichiers temporaires génér̀s lorsque vous utilisez une application, mais *ne supprime pas* l'application elle-même. Dans la *Figure 5*, par exemple, la suite de programmes *Applications - Office 2003* reste installée sur l'ordinateur, mais les fichiers temporaires générés par ce programme sont supprimés. Pour désinstaller des programmes à l'aide de **CCleaner**, veuillez vous référer à la section **Options avancées, Faq et questions récapitulatives** [114], **5.1 Comment désinstaller des programmes avec CCleaner**.

Sixième étape. **Cliquez** sur 

pour lancer la suppression des fichiers temporaires et activer la fenêtres suivante:

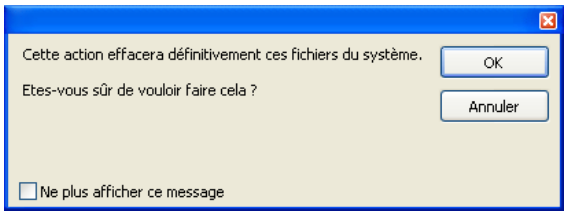
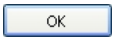

Cette action effacera définitivement ces fichiers du système.
Etes-vous sûr de vouloir faire cela ?
OK
Annuler
Ne plus afficher ce message

Figure 6: Boîte de dialogue de confirmation

Septième étape. **Cliquez** sur 

pour supprimer ces fichiers temporaires. Lorsque le processus de suppression est complété,le résultat s'affiche comme suit:

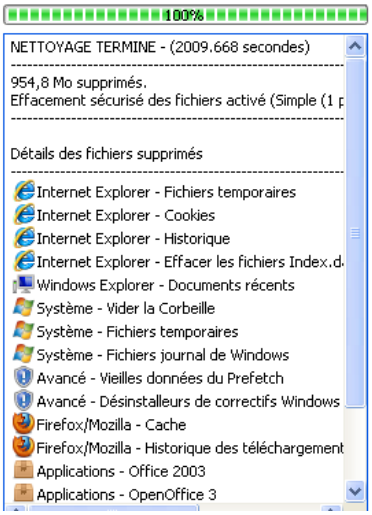

100%
NETTOYAGE TERMINE - (2009.668 secondes)
954,8 Mo supprimés.
Effacement sécurisé des fichiers activé (Simple (1 p
Détails des fichiers supprimés
Internet Explorer - Fichiers temporaires
Internet Explorer - Cookies
Internet Explorer - Historique
Internet Explorer - Effacer les fichiers Index.d
Windows Explorer - Documents récents
Système - Vider la Corbeille
Système - Fichiers temporaires
Système - Fichiers journal de Windows
Avancé - Vieilles données du Prefetch
Avancé - Désinstalleurs de correctifs Windows
Firefox/Mozilla - Cache
Firefox/Mozilla - Historique des téléchargement
Applications - Office 2003
Applications - OpenOffice 3

Figure 7: Le résultat de la suppression de fichiers temporaires

Vous avez réussi à supprimer les fichiers temporaires de *Windows* et de vos *Applications* avec **CCleaner**.

Comment nettoyer le Registre de Windows avec CCleaner

Sommaire des sections de cette page:

- **4.0 Avant de commencer**
- **4.1 Comment nettoyer le Registre de Windows avec CCleaner**
- **4.2 Comment restaurer un fichier de sauvegarde du registre**

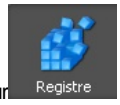
4.0 Avant de commencer

CCleaner vous permet également de nettoyer le **Registre de Windows**, une base de données où sont enregistrées vos configurations et les paramètres du matériel et des logiciels installés sur votre ordinateur. Chaque fois que vous modifiez la configuration du système, installez un logiciel ou exécutez une tâche de routine, ces modifications sont enregistrées dans le **Registre de Windows**.

Au fil du temps, le **Registre de Windows** accumule des données de configuration et de réglage désuètes, y compris des traces de programmes obsolètes. L'option *Registre* de **CCleaner** vous permet d'exécuter un scan du registre pour supprimer ces données inutiles, ce qui améliore le fonctionnement et la vitesse de votre système, en plus de protéger votre confidentialité et votre sécurité numérique.

Astuce: Un scan du **Registre de Windows** devrait être exécuté à tous les mois.

4.1 Comment nettoyer le Registre de Windows avec CCleaner

Première étape. **Cliquez** sur 

pour afficher la fenêtre suivante:

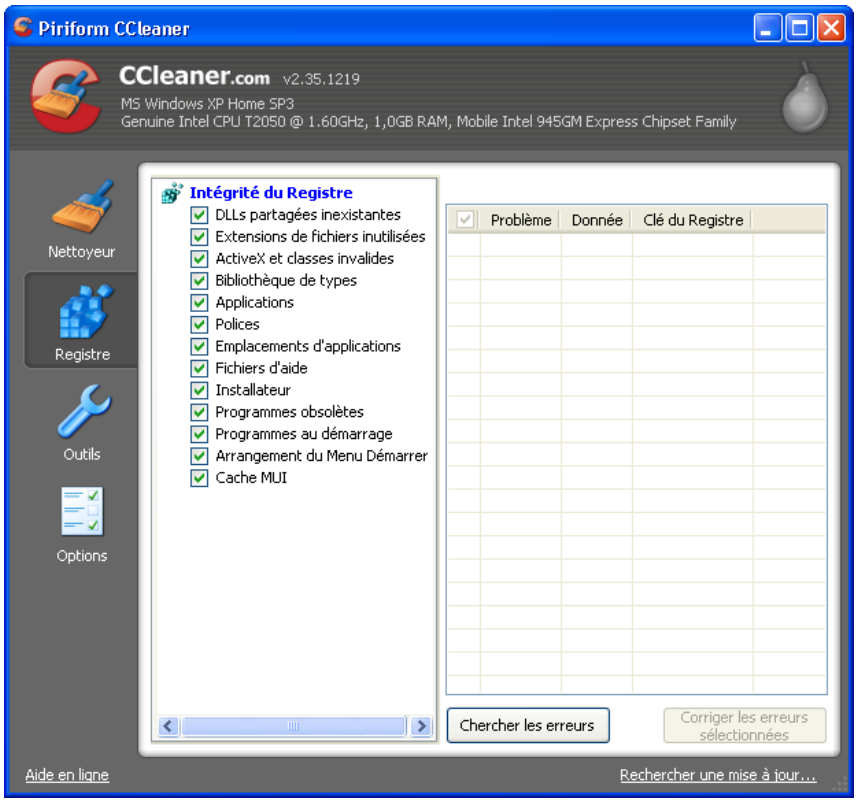


Figure 1: L'interface de CCleaner en mode Registre

La fenêtre *Registre* de **CCleaner** est divisée en deux panneaux: la liste *Intégrité du Registre* et le panneau où s'affiche l'information concernant les problèmes trouvés.

Deuxième étape. **Cochez** tous les items de la liste *Intégrité du registre*, puis **cliquez** sur Chercher les erreurs pour lancer le scan du registre et détecter d'éventuels problèmes à corriger; après un certain temps, le résultat du scan s'affiche comme suit:

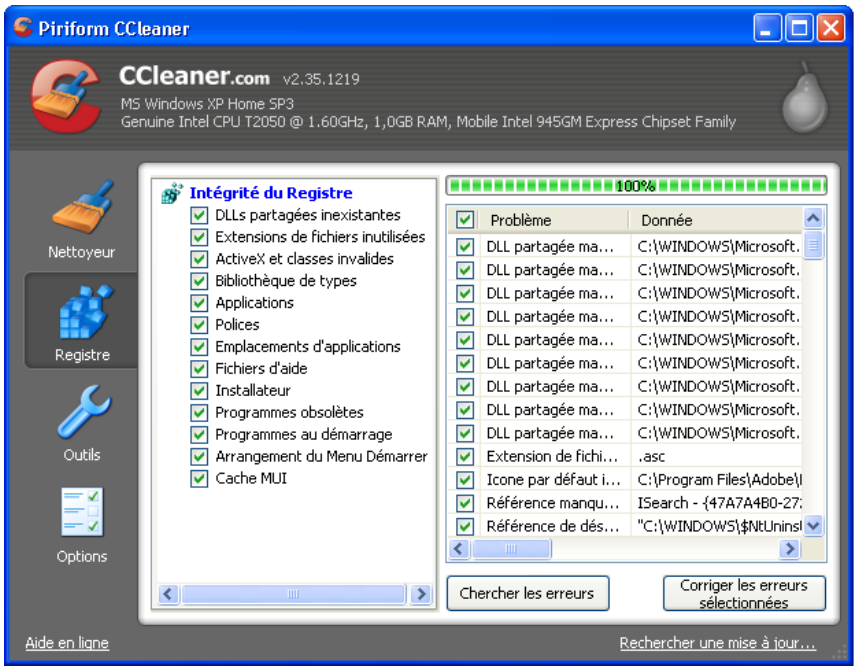


Figure 2: La panneau des résultats affichant une liste de problèmes à corriger

En guise de mesure de précaution avant de corriger le **Registre Windows**, le programme vous proposera de créer une copie de sauvegarde du registre. Si un quelconque problème survient suite au nettoyage du **Registre de Windows**, il vous sera possible de restaurer le **Registre de Windows** à son état précédent en utilisant cette copie de sauvegarde.

Troisième étape. **Cliquez** sur Corriger les erreurs sélectionnées pour afficher la boîte de dialogue de confirmation illustrée ci-dessous:

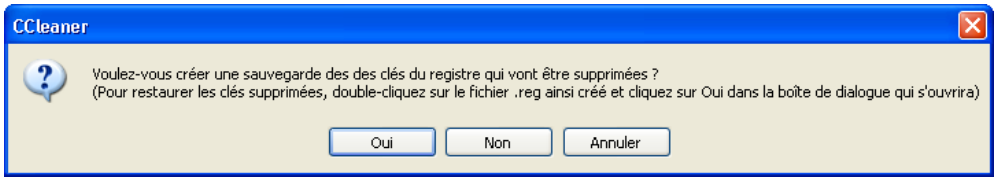

CCleaner
Voulez-vous créer une sauvegarde des des clés du registre qui vont être supprimées ?
(Pour restaurer les clés supprimées, double-cliquez sur le fichier .reg ainsi créé et cliquez sur Oui dans la boîte de dialogue qui s'ouvrira)
Oui
Non
Annuler

Figure 3: La boîte de dialogue de confirmation

Commentaire: Si vous oubliez l'emplacement de votre copie de sauvegarde, vous n'avez qu'à effectuer une recherche de l'extension de fichier *.reg*.

Quatrième étape. **Cliquez** sur [Oui] pour créer une copie de sauvegarde des clés du registre et afficher la fenêtre suivante:

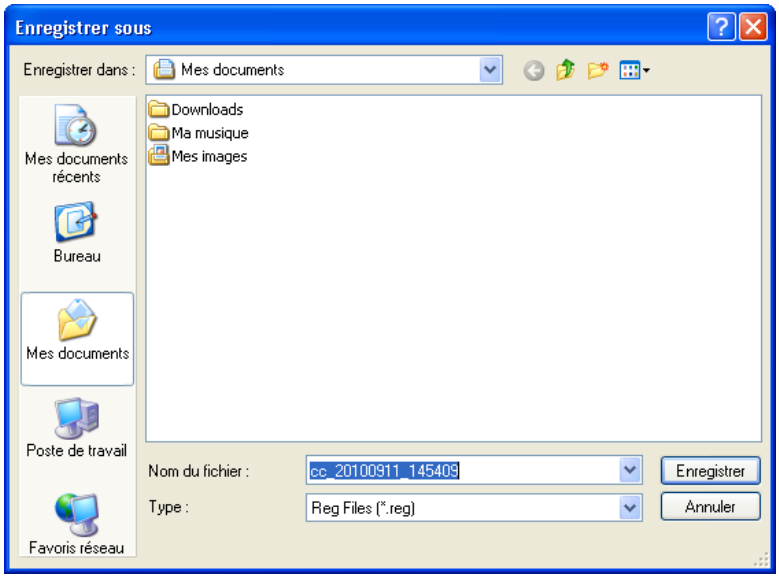


Figure 4: La fenêtre Enregistrer sous

Cinquième étape. **Cliquez** sur [Enregistrer], après avoir choisi un emplacement pour votre copie de sauvegarde, pour afficher la fenêtre suivante:

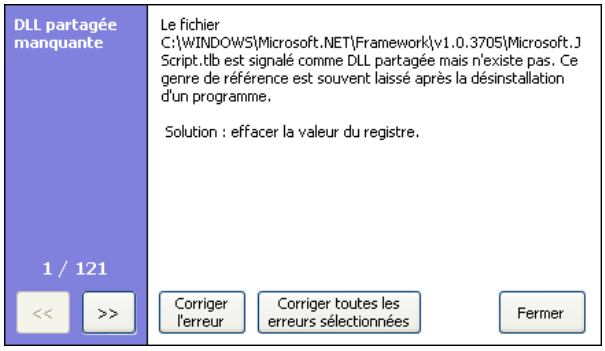

DLL partagée manquante
Le fichier C:\WINDOWS\Microsoft.NET\Framework\v1.0.3705\Microsoft.JScript.tlb est signalé comme DLL partagée mais n'existe pas. Ce genre de référence est souvent laissé après la désinstallation d'un programme.
Solution : effacer la valeur du registre.
1 / 121
<<
>>
Corriger l'erreur
Corriger toutes les erreurs sélectionnées
Fermer

Figure 5: La boîte de dialogue Corriger l'erreur/Corriger toutes les erreurs sélectionnées

Les utilisateurs experts ou avancés apprécieront la possibilité de corriger certaines erreurs et d'en ignorer d'autres, selon leur préférences. Il est recommandé aux utilisateurs moyens ou intermédiaires de corriger toutes les erreurs sélectionnées.

Sixième étape. **Cliquez** sur [<<] ou [>>] pour afficher chaque erreur, puis **cliquez** sur [Corriger l'erreur] pour corriger uniquement celles que vous souhaitez corriger.

Septième étape. **Cliquez** sur [Corriger toutes les erreurs sélectionnées] pour corriger toutes les erreurs sélectionnées.

Le **Registre de Windows** a été nettoyé avec succès.

Astuce: Répétez les **étapes 3** à **6** jusqu'à ce qu'il n'y ait plus aucune erreur à corriger.*

4.2 Comment restaurer un fichier de sauvegarde du registre

Si vous avez l'impression que le nettoyage du **Registre de Windows** a occasionné un problème avec le fonctionnement normal de votre système, le fichier de sauvegarde que vous avez créé aux **étapes 3** à **5** de la section **4.1** peut être utilisée pour restaure le registre à son état précédent et ainsi réduire l'interférence avec votre système.

Pour restaurer le registre, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Démarrer > Exécuter** pour afficher la boîte de dialogue *Exécuter*, puis **saisissez** *regedit*, comme suit:

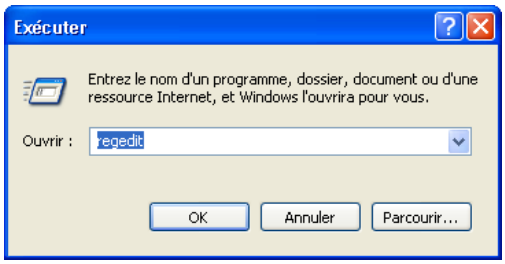


Figure 6: La boîte de dialogue Exécuter

Deuxième étape. **Cliquez** sur OK pour afficher la fenêtre suivante:

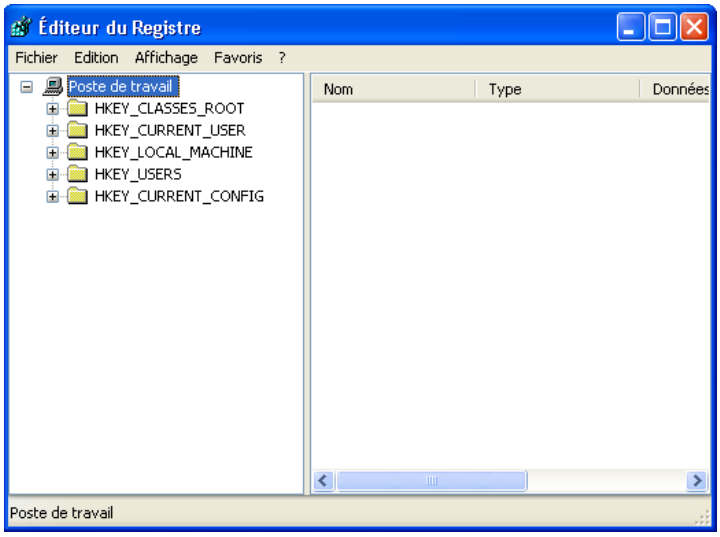


Figure 7: L'Éditeur du registre

Troisième étape. **Sélectionnez Fichier > Importer** dans la barre de menu pour afficher la fenêtre *Importer un fichier du registre*, puis **sélectionnez** cc_20100911_145409.

Quatrième étape. **Cliquez** sur Ouvrir pour afficher la boîte de dialogue suivante:

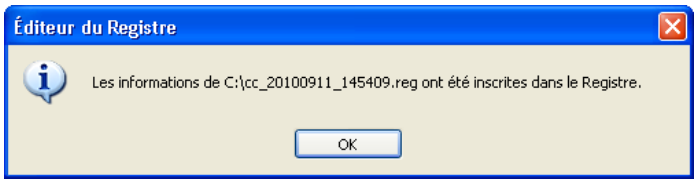


Figure 8: Une autre Boîte de dialogue de l'Éditeur du registre confirmant que le fichier de sauvegarde a été restauré

Cinquième étape. **Cliquez** sur OK pour finaliser la restauration du fichier de sauvegarde du registre.

Options avancées, faq et questions récapitulatives

Sommaire des sections de cette page:

- **5.0 Options avancées**
- **5.1 Comment désinstaller des programmes avec CCleaner**
- **5.2 Comment désactiver le lancement au démarrage des programmes avec CCleaner**
- **5.3 Comment nettoyer l'espace libre de vos disques durs avec CCleaner**
- **5.4 Faq**
- **5.5 Questions récapitulatives**

5.0 Options avancées

Deux autres fonctions de **CCleaner** peuvent améliorer considérablement l'efficacité générale de votre système: les fonctions *Désinstallation de programmes* et *Démarrage*. Ces fonctions sont décrites dans les sections suivantes. Vous apprendrez également comment *Nettoyer*, ou *Effacer*, l'espace libre de vos disques durs.

5.1 Comment désinstaller des programmes avec CCleaner

Important: Assurez-vous que le programme à supprimer ou désinstaller n'est pas essentiel au bon fonctionnement de votre ordinateur.

En supprimant des logiciels préalablement installés, qui sont désormais inutilisés ou superflus, avant de lancer **CCleaner**, il est possible que vous en supprimiez également les fichiers temporaires. Cela peut réduire le nombre de fichiers et dossiers temporaires èa supprimer, ainsi que la durée du processus de nettoyage.

La fonction *Désinstallation de programmes* de **CCLeaner** est semblable à la fonction **Ajout/Suppression de programmes** de **Microsoft Windows**. La fonction ** Désinstallation de programmes** liste les programmes plus clairement et plus rapidement.

Pour entamer la désinstallation des programmes obsolètes, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur ou **sélectionnez Démarrer > Programmes > CCleaner** pour activer l'interface principale de *Piriform CCleaner*.

Deuxième étape. **Cliquez** sur

, puis **cliquez** sur

pour afficher la fenêtre ci-dessous:

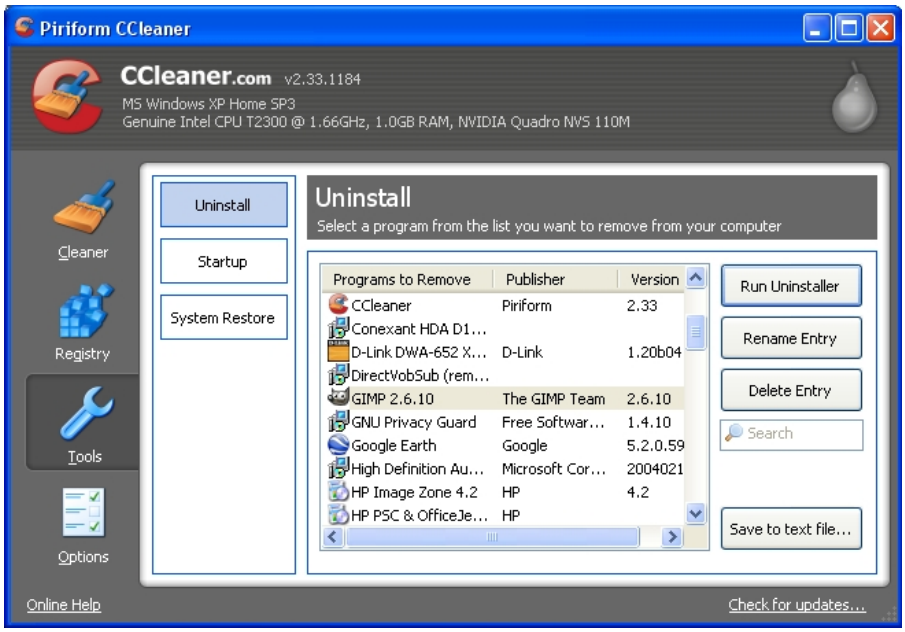
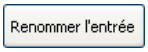


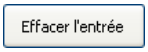
Figure 1: L'option Outils affichant le panneau Désinstallation de programmes

Troisième étape. **Sélectionnez** un programme dans la liste *Programmes*, puis **cliquez** sur

pour désinstaller le programme sélectionné.

Astuce: Les utilisateurs avancés ou experts trouveront sans doute les fonctions *Renommer l'entrée* et *Effacer l'entrée* utiles pour garder confidentielle l'existence de certains logiciels. Ces deux fonctions vous assurent que personne d'autre que vous ne puisse détecter l'existence de ce programme, ce qui le protège des parties potentiellement hostiles ou malveillantes qui pourraient utiliser la fonction **Ajout/Suppression de programmes** de **Microsoft Windows** ou celle de **CCleaner** pour les afficher.

Cliquez sur 

pour renommer le programme. Autrement, vous pouvez **cliquer** sur 

pour supprimer le programme de la liste, mais *sans pour autant* le supprimer

5.2 Comment désactiver le lancement au démarrage des programmes avec CCleaner

Un programme lancé au démarrage est réglé pour se lancer automatiquement lorsque vous allumez votre ordinateur. Les programmes lancés automatiquement peuvent être exigeants envers les ressources limitées du système et ainsi ralentir l'ordinateur au démarrage.

Première étape. **Cliquez** sur

, puis **cliquez** sur

pour afficher la fenêtre suivante:

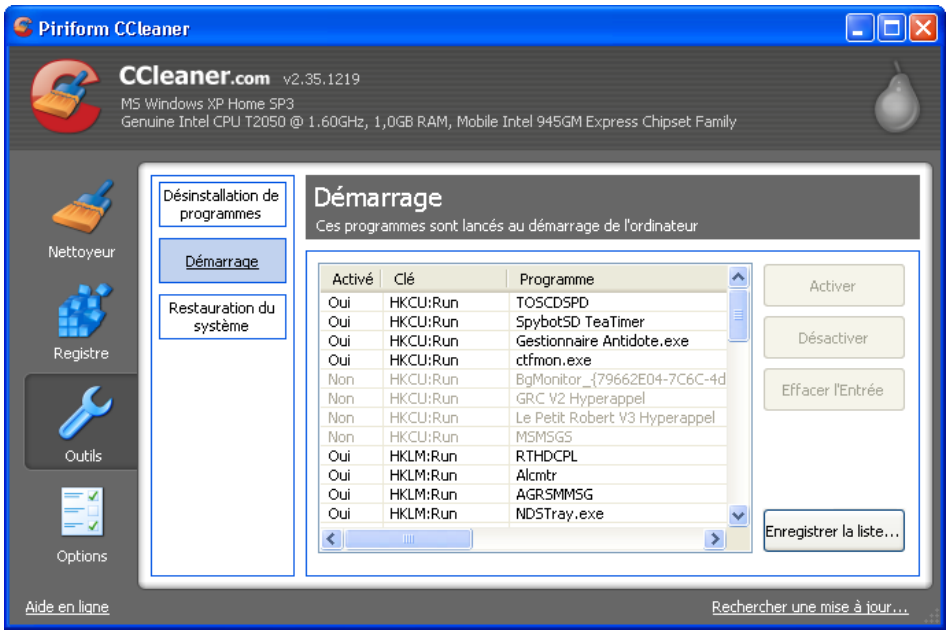


Figure 12: L'option Outils affichant le panneau Démarrage

Deuxième étape. **Sélectionnez** un programme dans la liste du panneau *Démarrage*, puis **cliquez** sur Désactiver pour désactiver le lancement au démarrage du programme.

5.3 Comment nettoyer l'espace libre de vos disques durs avec CCleaner

Dans le système d'exploitation **Windows**, la suppression d'un fichier ne fait que supprimer la référence à ce fichier sans supprimer les données elles-mêmes. Bien que l'espace occupé par ces données sur le disque sur sera éventuellement écrasé par d'autres fichiers, une personne experte pourrait être en mesure de reconstruire le fichier en partie ou en entier. Cependant, vous pouvez empêcher cela en nettoyant, ou effaçant, l'espace libre de votre disque dur. **CCleaner** vous permet également de nettoyer la **Master File Table (MFT)**.

La **Master File Table (MFT)** est un index de tous les noms de fichier, leur emplacement et autres renseignements connexes. Lorsque **Microsoft Windows** supprime un fichier, le système marque ce fichier comme 'supprimé' uniquement pour des raisons de rendement. L'entrée **MFT** du fichier, ainsi que le contenu du fichier, demeure sur le disque dur.

Commentaire: Le nettoyage du disque dur et de la **MTP** requiert une somme considérable de temps, et le temps requis dépend du nombre de passages déterminé.

Avant d'entamer le nettoyage de l'espace libre du disque dur et de la **MTP**, certaines options doivent être réglées dans les panneaux *Options* > *Paramètres* et *Nettoyeur*.

Pour choisir le disque que vous souhaitez nettoyer, suivez les étapes énumérées ci-dessous:

Première étape. **Faites dérouler** la liste vers le bas et **cochez** l'option *Effacement sécurisé (lent)*, puis **sélectionnez** DOD 5220.22-M (3 passages) si cela n'est pas déjà fait.

Deuxième étape. **Cliquez** sur Options, puis sur Paramètres pour afficher le panneau *Paramètres*.

Troisième étape. **Cochez** les options *Lecteurs sur lesquels nettoyer l'espace libre* et *Nettoyer l'espace libre de la MFT*, tel qu'illustré ci-dessous:

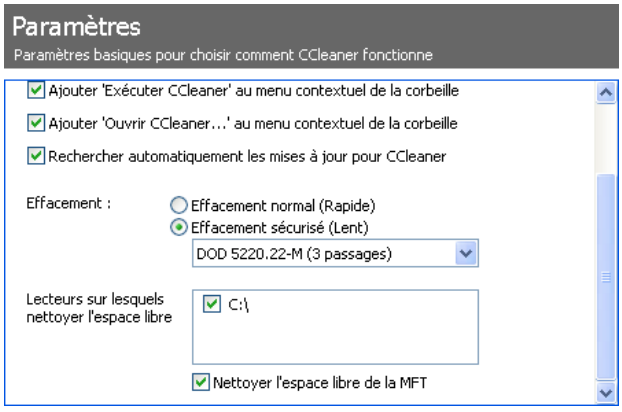

Paramètres
Paramètres basiques pour choisir comment CCleaner fonctionne
Ajouter 'Exécuter CCleaner' au menu contextuel de la corbeille
Ajouter 'Ouvrir CCleaner...' au menu contextuel de la corbeille
Rechercher automatiquement les mises à jour pour CCleaner
Effacement :
Effacement normal (Rapide)
Effacement sécurisé (Lent)
DOD 5220.22-M (3 passages)
Lecteurs sur lesquels nettoyer l'espace libre
C:\
Nettoyer l'espace libre de la MFT

Figure 3: Le panneau Paramètres avec les deux options de nettoyage sélectionnés

Quatrième étape. **Cliquez** sur

pour afficher l'interface principale de *Piriform CCleaner*.

Commentaire: La prochaine étape est optionnelle si vous avez déjà activé cette option lorsque vous avez exécuté un nettoyage de routine de vos fichiers temporaires.

Astuce: Souvenez-vous de fermer tous les programmes ouverts avant de lancer le processus de nettoyage. Si laissez certains programmes ouverts, **CCleaner** ne sera peut-être pas en mesure de supprimer tous les fichiers temporaires qui y sont associés.

Cinquième étape. **Faites dérouler** l'onglet *Windows* vers le bas jusqu'à la section *Avancé*, puis **cochez** l'option *Nettoyer l'espace libre* pour afficher la fenêtre d'avertissement ci-dessous:

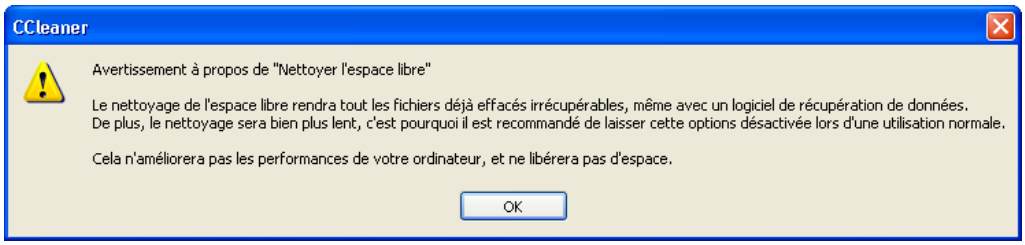
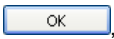
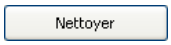

CCleaner
Avertissement à propos de "Nettoyer l'espace libre"
Le nettoyage de l'espace libre rendra tout les fichiers déjà effacés irrécupérables, même avec un logiciel de récupération de données.
De plus, le nettoyage sera bien plus lent, c'est pourquoi il est recommandé de laisser cette options désactivée lors d'une utilisation normale.
Cela n'améliorera pas les performances de votre ordinateur, et ne libérera pas d'espace.
OK

Figure 4: La boîte de dialogue d'avertissement

Sixième étape. **Cliquez** sur 

, puis **cliquez** sur 

pour afficher la fenêtre suivante:

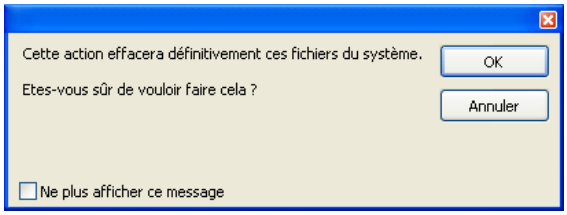
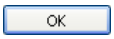

Cette action effacera définitivement ces fichiers du système.
Etes-vous sûr de vouloir faire cela ?
OK
Annuler
Ne plus afficher ce message

Figure 5: La boîte de dialogue de confirmation

Septième étape. **Cliquez** sur 

pour entamer le nettoyage de l'espace libre de votre disque dur, et de la **Master File Table**.

5.4 Faq

Elena et Nikolai trouvent **CCleaner** facile à utiliser, mais ils ont encore quelques questions sur son emploi:

***Q**: Si je désinstalle **CCleaner**, est-ce que le matériel que j'ai supprimé restera effacé?*

***A**: Oui. Si tu as configuré et utilisé **CCleaner** adéquatement, les fichiers supprimés sont éliminés définitivement.*

***Q**: Si je sauvegarde **CCleaner** sur ma clé USB, puis-je l'utiliser sur l'ordinateur d'un café Internet pour effacer les traces du travail que j'y ai effectué ? Y a t-il une raison pour laquelle je ne devrais pas l'utiliser de cette façon?*

***A**: Oui! Il existe une version portable de **CCleaner**. Il faut consulter la section **CCleaner - Portable** de la page de téléchargement **www.piriform.com/ccleaner/builds** [109]. Si le café Internet te permet d'exécuter des programmes à partir d'une clé USB, alors oui, il est possible d'utiliser **CCleaner** pour effacer les traces du travail que tu as effectué sur cet ordinateur. Par contre, n'oublie pas que ton activité au café Internet est peut-être contrôlée. De plus, tu risque d'infecter ta clé USB en la connectant à l'ordinateur du café Internet.*

***Q**: Si je n'utilise qu'un seul passage de **CCleaner**, est-ce qu'une autre personne sera en mesure de récupérer mes données? Et si j'en utilise sept?*

***A**: Excellente question! Plus le nombre de passages exécutés est élevé pour effacer des données, moins il y a de chance qu'une tierce personne ne les récupère : cependant, le processus de nettoyage sera plus long.*

***Q**: Si je nettoie le **Registre de Windows**, est-ce que toutes les traces des programmes que j'ai temporairement chargés sur mon ordinateur et ensuite enlevés seront effacés?*

***A**: Oui. Tu devrais aussi effectuer le nettoyage des fichiers temporaires en plus de nettoyer le **Registre de Windows**. Ainsi, tu effaceras toute trace de logiciels (et du coup, des opérations que tu y as faites) qui n'existent plus sur ton ordinateur. Cependant, si tu n'a que très peu de temps, le nettoyage du **Registre de Windows** est un bon départ!*

5.5 Questions récapitulatives

- Quelle information CCleaner efface-t-il de votre ordinateur?
- Comment procède-t-il?
- Quelle différence y a-t-il entre le nombre de passes que vous choisissez au moment d'écraser des données de façon sécuritaire?
- Qu'est-ce que le **Registre de Windows**, et pourquoi est-il recommandé de le nettoyer?
- Que devriez-vous faire avant de nettoyer **Registre de Windows**?

Riseup - service de courriel sécurisé

Short Description:

RiseUp est un collectif dont l'objectif premier est d'offrir des services d'hébergement Web, de listes de distribution et de courrier électronique privés et sécurisés à des individus et organismes qui luttent pour la justice sociale.

Site Internet

https://riseup.net/ [115]

Configuration requise

- Une connexion Internet
- **RiseUp** offre une fonctionnalité accrue avec le navigateur **Firefox**

Licence

- Gratuiciel (*Freeware*)

Lecture préalable

- Livret pratique Security in-a-box, chapitre **7. Préserver la confidentialité de vos communications sur Internet** [116]

Niveau: 1 : Débutant, **2 : Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

Temps d'apprentissage: 20 minutes

Ce que vous apportera l'utilisation de cet outil:

- L'accès à un compte de courrier électronique sans publicité, autogéré par une communauté militante.
- La possibilité d'accéder à votre courrier électronique par Internet ou à l'aide d'un client de messagerie, et de communiquer confidentiellement par courrier électronique via une connexion chiffrée.
- La capacité de modifier votre adresse de courriel, de déterminer la taille de votre boîte de courriel et d'inviter d'autres personnes à joindre **RiseUp**

Autres services de courrier électronique:

Même si **RiseUp** offre un service sécurisé, géré par un collectif de confiance qui accorde beaucoup d'importance à la sécurité numérique, un service de courrier électronique inhabituel pourrait attirer une attention non désirable. Dans certaines situations, il peut être plus avantageux de passer inaperçu en optant plutôt pour un service de courriel populaire dans votre pays. L'important est de prendre une décision éclairée sans compromettre vos besoins élémentaires en matière de sécurité. Voici quelques considérations à tenir en compte lorsque vous choisissez un service de courrier électronique:

1. Le service permet-il d'utiliser des canaux chiffrés (comme *https*, et d'autres versions chiffrées SSL des protocoles comme IMAP, POP3 et SMTP) pour transférer l'information (y compris les détails de connexion et le contenu des messages); et le service présente-t-il des problèmes de chiffrement (par exemple, des problèmes liés aux certificats de chiffrement)?

2. Les serveurs de courriel sont-ils gérés de façon sûre et sécuritaire? Sont-ils gérés par des professionnels qui emploient les pratiques exemplaires pour protéger vos données? Leur faites-vous confiance pour *ne pas* donner l'accès à vos données, pour quelque raison que ce soit (commerciale, politique, religieuse, etc.), à des tierces parties?

3. Connaissez-vous l'emplacement géographique des serveurs; sous quelle juridiction territoriale se trouvent-ils; ou dans quel pays la compagnie est-elle située? Savez-vous de quelle façon ces renseignements peuvent avoir un impact sur la confidentialité et la sécurité de vos communications par courrier électronique?

Dans certaines parties du monde, **Google Mail** peut s'avérer une bonne alternative à **RiseUp**, puisque ce service est très répandu et permet de passer inaperçu sans pour autant compromettre la sécurité de vos communications (étant donné son caractère commercial).

1.1 À propos de cet outil

RiseUp est un collectif dont l'objectif premier est d'offrir des services d'hébergement Web, de listes de distribution et de courrier électronique privés et sécurisés à des individus et organismes qui luttent pour la justice sociale. Puisque leurs services sont gratuits, les comptes de courriel offerts par **RiseUp** sont considérablement plus petits que ceux qu'offrent les fournisseurs de services non sécurisés et/ou soumis aux intérêts publicitaires. De plus, un nouveau compte ne peut être enregistré que par une personne qui a reçu des codes d'invitation de la part de membres existants ou de participants au projet **Digital Security**.

RiseUp fonctionne exclusivement avec le protocole **Secure Sockets Layer** (**SSL**), ce qui assure une connexion sécurisée entre votre ordinateur et leur serveur. Ce niveau de sécurité est maintenu lorsque vous relevez votre courrier électronique à l'aide d'un client de messagerie, avec une connexion sécurisée utilisant **POP**, **IMAP** ou **SMTP** (différents protocoles spéciaux utilisés par des programme de messagerie pour télécharger votre courrier électronique).

RiseUp est compatible avec **Mozilla Thunderbird**. Pour apprendre à configurer **Mozilla Thunderbird** pour accéder à votre compte **RiseUp**, veuillez consulter le Guide pratique **Thunderbird** [117].

Comment créer un compte Riseup

Sommaire des sections de cette page:

- **2.0 Les différentes méthodes d'enregistrement d'un compte RiseUp**
- **2.1 Le formulaire d'Information sur le compte**
- **2.2 Le formulaire de Mot de passe**
- **2.3 Le formulaire d'Entraide**
- **2.4 Le formulaire d'Activation**

2.0 Les différentes méthodes d'enregistrement d'un compte RiseUp

RiseUp offre trois méthodes différentes pour enregistrer un compte de courriel. Chaque méthode exige un investissement variable de temps et d'effort.

1) Des individus et/ou des organismes sont invités par deux personnes disposant déjà de comptes **RiseUp**. Cette méthode implique que vous receviez un code d'invitation de la part de chacune de ces personnes. Pour savoir comment ces codes sont générés, consultez la section **4.3 La page Invitations** [118]

2) Effectuer une demande directement à l'équipe **RiseUp** pour obtenir un compte. Cette méthode exige beaucoup de patience. N'oubliez pas que **RiseUp** repose principalement sur l'enthousiasme et la bonne volonté de ses bénévoles!

3) Les participants au programme de formation du **Digital Security Project** recevront un code d'enregistrement avec leur copie de la trousse à outils **Security in-a-box**.

Après avoir reçu vos codes d'invitation, suivez les étapes énumérées ci-dessous pour enregistrer votre compte **RiseUp** gratuit :

Première étape. **Saisissez https://mail.riseup.net** [119] dans la barre d'adresse de votre navigateur pour activer le site Internet de **RiseUp**, illustré ci-dessous:

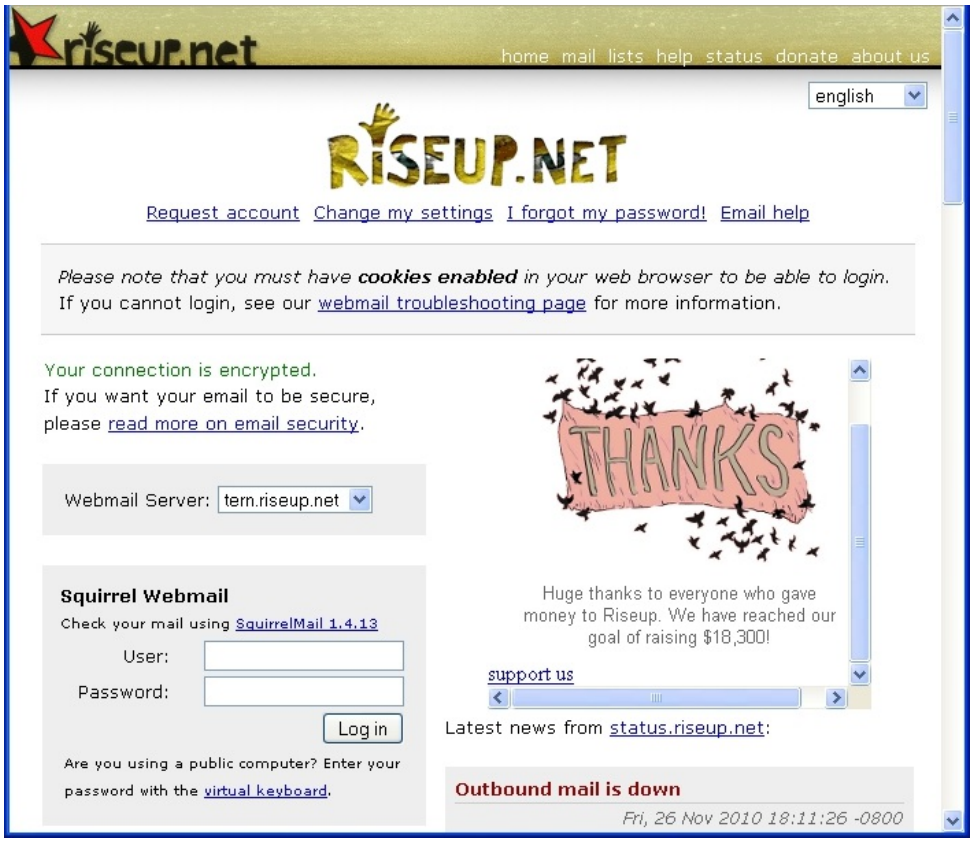

riseup.net
home mail lists help status donate about us
english
RISEUP.NET
Request account Change my settings I forgot my password! Email help
Please note that you must have cookies enabled in your web browser to be able to login.
If you cannot login, see our webmail troubleshooting page for more information.
Your connection is encrypted.
If you want your email to be secure,
please read more on email security.
Webmail Server: tern.riseup.net
Squirrel Webmail
Check your mail using SquirrelMail 1.4.13
User:
Password:
Log in
Are you using a public computer? Enter your password with the virtual keyboard.
THANKS
Huge thanks to everyone who gave money to Riseup. We have reached our goal of raising $18,300!
support us
Latest news from status.riseup.net:
Outbound mail is down
Fri, 26 Nov 2010 18:11:26 -0800

Figure 1: La page https://mail.riseup.net/

Commentaire: Le ***s*** dans l'adresse *https://* Cela indique que vous communiquez via une connexion *Secure Socket Laye* (*SSL*), et le message texte en vert Your connection is encrypted est affiché au dessus des zones de texte servant à la connexion.

Pour plus de renseignements à ce sujet, veuillez consulter le chapitre **7. Préserver la confidentialité de vos communications sur Internet** [116] du **livret pratique**, ou visitez **https://help.riseup.net/security** [120].

Deuxième étape. **Cliquez** sur Request account pour afficher la page *Demander un nouveau compte* illustrée ci-dessous :

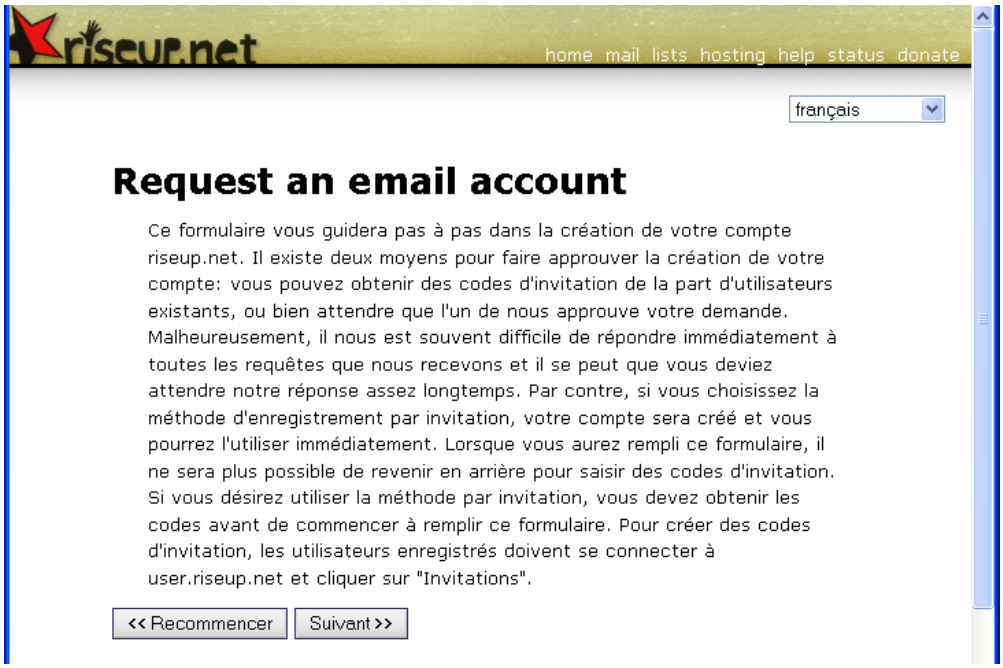

riseup.net
home mail lists hosting help status donate
français
Request an email account
Ce formulaire vous guidera pas à pas dans la création de votre compte riseup.net. Il existe deux moyens pour faire approuver la création de votre compte: vous pouvez obtenir des codes d'invitation de la part d'utilisateurs existants, ou bien attendre que l'un de nous approuve votre demande. Malheureusement, il nous est souvent difficile de répondre immédiatement à toutes les requêtes que nous recevons et il se peut que vous deviez attendre notre réponse assez longtemps. Par contre, si vous choisissez la méthode d'enregistrement par invitation, votre compte sera créé et vous pourrez l'utiliser immédiatement. Lorsque vous aurez rempli ce formulaire, il ne sera plus possible de revenir en arrière pour saisir des codes d'invitation. Si vous désirez utiliser la méthode par invitation, vous devez obtenir les codes avant de commencer à remplir ce formulaire. Pour créer des codes d'invitation, les utilisateurs enregistrés doivent se connecter à user.riseup.net et cliquer sur "Invitations".
<< Recommencer
Suivant >>

Figure 2: La page Demander un nouveau compte de RiseUp

Étape optionnelle. **Sélectionnez** votre langue d'usage dans le menu défilant qui se trouve à droite de l'écran, si nécessaire.

Troisième étape. **Cliquez** sur Suivant >> pour afficher la page **RiseUp** *À propos de notre service de courriel*.

Important: Vous *devez* cocher les options suivantes afin de poursuivre le processus de création d'un compte **RiseUp**.

Quatrième étape. Après avoir lu les politiques de **RiseUp**, **cochez** les options *J'accepte le contrat social de riseup.net*, *J'accepte la politique de confidentialité de riseup.net* et *J'accepte les termes d'utilisation de riseup.net*.

Cinquième étape. **Cliquez** sur Suivant >> pour commencer à créer votre compte **RiseUp** en remplissant les formulaires : *Information sur le compte*, *Mot de passe*, *Entraide* et *Activation*.

2.1 Le formulaire d'Information sur le compte

Sixième étape. **Saisissez** un nom d'utilisateur pour votre compte. Ce nom sera utilisé pour vous connecter au site et vous servira d'adresse de courriel (par exemple, saisissez le nom "thierryfictif" si vous souhaitez que votre adresse de courriel soit **thierryfictif@riseup.net**).

Important: 'utilisez pas d'espace, de virgules ou de point final dans le nom d'utilisateur.

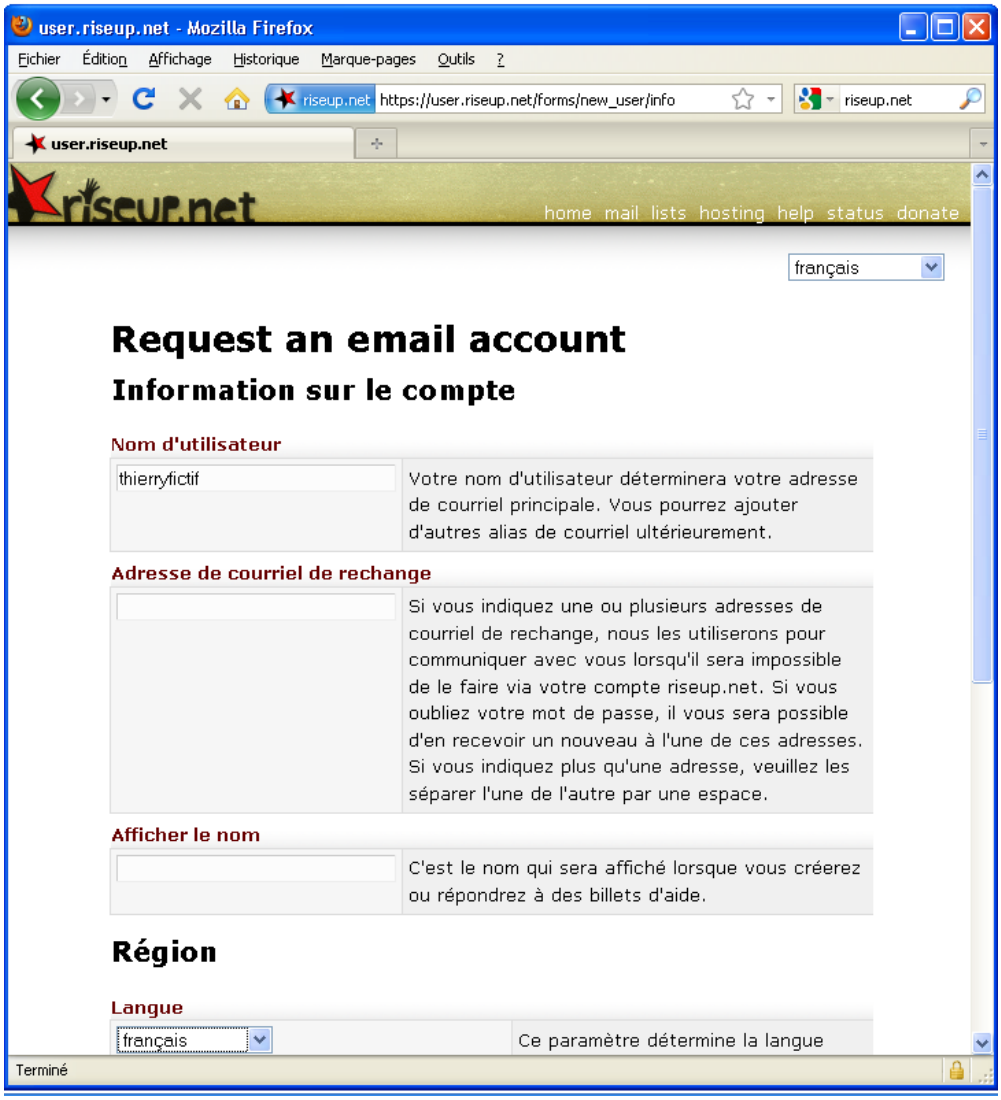

user.riseup.net - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
riseup.net https://user.riseup.net/forms/new_user/info
riseup.net
user.riseup.net
riseup.net
home mail lists hosting help status donate
français
Request an email account
Information sur le compte
Nom d'utilisateur
thierryfictif
Votre nom d'utilisateur déterminera votre adresse de courriel principale. Vous pourrez ajouter d'autres alias de courriel ultérieurement.
Adresse de courriel de rechange
Si vous indiquez une ou plusieurs adresses de courriel de rechange, nous les utiliserons pour communiquer avec vous lorsqu'il sera impossible de le faire via votre compte riseup.net. Si vous oubliez votre mot de passe, il vous sera possible d'en recevoir un nouveau à l'une de ces adresses. Si vous indiquez plus qu'une adresse, veuillez les séparer l'une de l'autre par une espace.
Afficher le nom
C'est le nom qui sera affiché lorsque vous créerez ou répondrez à des billets d'aide.
Région
Langue
français
Ce paramètre détermine la langue
Terminé

Figure 3: Un formulaire d'Information sur le compte dûment rempli

Septième étape. **Cliquez** sur Suivant >> après avoir choisi un nom d'utilisateur original, pour afficher la page du formulaire *Mot de passe*.

Commentaire: Si ce nom d'utilisateur existe déjà, vous devrez en créer un nouveau.

2.2 Le formulaire de Mot de passe

Dans ce formulaire, vous *devez* créer une question de sécurité et la réponse assortie, ainsi qu'un bon mot de passe afin de protéger la connexion à votre compte, faute de quoi il ne vous sera pas permis de poursuivre le processus de création du compte. **RiseUp** vous recommande de créer une question de sécurité comme recours d'urgence au cas où vous oublieriez votre mot de passe. Malheureusement, cette mesure bien intentionnée constitue une vulnérabilité.

Par exemple, un adversaire potentiel n'aurait en théorie qu'à deviner la bonne réponse pour intercepter le nouveau mot de passe qui vous serait alors envoyé. Il est donc fortement *recommandé* d'éliminer complètement la possibilité de deviner la réponse à votre question secrète en *sabotant* ces deux zones de texte, tel qu'illustré dans l'exemple ci-dessous :

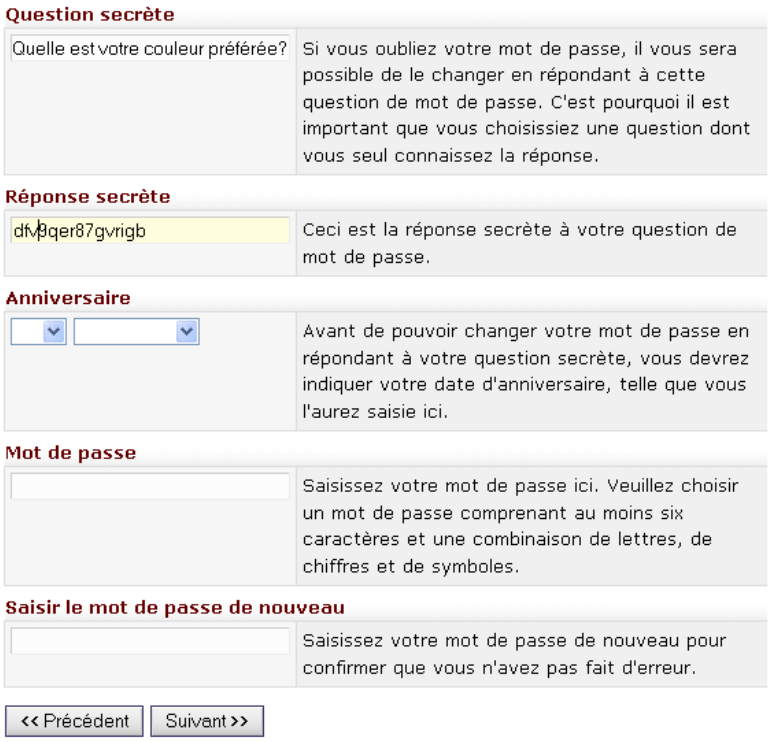

Question secrète
Quelle est votre couleur préférée?
Si vous oubliez votre mot de passe, il vous sera possible de le changer en répondant à cette question de mot de passe. C'est pourquoi il est important que vous choisissiez une question dont vous seul connaissez la réponse.
Réponse secrète
dfv9qer87gvrigb
Ceci est la réponse secrète à votre question de mot de passe.
Anniversaire
Avant de pouvoir changer votre mot de passe en répondant à votre question secrète, vous devrez indiquer votre date d'anniversaire, telle que vous l'aurez saisie ici.
Mot de passe
Saisissez votre mot de passe ici. Veuillez choisir un mot de passe comprenant au moins six caractères et une combinaison de lettres, de chiffres et de symboles.
Saisir le mot de passe de nouveau
Saisissez votre mot de passe de nouveau pour confirmer que vous n'avez pas fait d'erreur.
<< Précédent
Suivant >>

Figure 4: Une exemple de question et réponse sabotées dans le formulaire de Mot de passe

Attention: Cela signifie également qu'il sera pratiquement impossible de réinitialiser votre mot de passe. Vous devrez vous en rappeler! Si cette méthode n'est pas vraiment pratique, ça demeure l'option la plus sûre.

Le mot de passe pour votre compte **RiseUp** est l'élément le plus important en ce qui à trait à la sécurité du comte. Vous devez choisir un mot de passe fort. Pour plus d'information à ce sujet, veuillez consulter le chapitre **3. Créer et sauvegarder des mots de passe sûrs** [53] du livret pratique, ainsi que le Guide pratique **KeePass** [77].

Mot de passe
Saisissez votre mot de passe ici. Veuillez choisir un mot de passe comprenant au moins six caractères et une combinaison de lettres, de chiffres et de symboles.
Saisir le mot de passe de nouveau
Saisissez votre mot de passe de nouveau pour confirmer que vous n'avez pas fait d'erreur.

Figure 5: Les zones de texte du formulaire Mot de passe dûment remplies

Huitième étape. **Cliquez** sur Suivant >> pour afficher la page du formulaire d'*Entraide*.

2.3 Le formulaire d'Entraide

En ce qui concerne l'aide financière et le bénévolat, **RiseUp** *dépend entièrement* de la générosité et de la gentillesse d'étrangers. Bien que leur demande de soutien financier soit tout à fait légitime et nécessaire, **RiseUp** encourage les utilisateurs à investir leur argent dans des projets locaux en faveur de la justice sociale. Il n'en tient qu'à vous de décider si vous ou votre organisme êtes en mesure d'offrir une contribution financière.

Commentaire: Votre décision n'affectera en rien le processus d'enregistrement de votre compte. Vous pourrez continuer à créer votre compte **RiseUp** gratuitement.

fr, mutual_aid
Ce service n'est pas gratuit. Il faut beaucoup de temps et d'argent pour maintenir riseup.net en vie. Dans un contexte où la surveillance est omniprésente et la publicité ciblée, nous croyons qu'il est plus important que jamais que les mouvements de libération soient en mesure de maîtriser leur propres moyens de communication. Veuillez contribuer, dans la mesure de vos moyens, à faire en sorte que nos serveurs fonctionnent et que nous puissions développer nos services. Vous ne recevrez pas un meilleur service si vous faites un don, mais votre karma vous remerciera. Pour des raisons de sécurité, nous n'enregistrons pas les dons. Cependant, nous vous enverrons des aide-mémoire selon la configuration que vous spécifiez ici.
Fréquence du don
jamais
À quelle fréquence souhaitez-vous faire un don?
Montant du don
0.0
Combien? Si vous vivez dans le Sud ou dans un contexte défavorisé, veuillez contribuer à des projets locaux plutôt qu'à Riseup.net. Merci.
<< Précédent
Suivant >>

Figure 6: Le formulaire fr, Entraide

Neuvième étape. **Cliquez** sur Suivant >> pour afficher le formulaire *Activation*.

2.4 Le formulaire d'Activation

C'est dans le formulaire *Activation* que vous êtes invité à saisir vos codes d'activation.

Dixième étape. **Saisissez** les deux *codes d'invitation* dans les zones de texte appropriées.

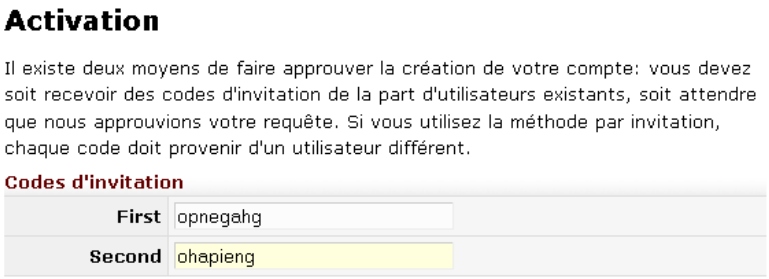

Activation
Il existe deux moyens de faire approuver la création de votre compte: vous devez soit recevoir des codes d'invitation de la part d'utilisateurs existants, soit attendre que nous approuvions votre requête. Si vous utilisez la méthode par invitation, chaque code doit provenir d'un utilisateur différent.
Codes d'invitation
First
opnegahg
Second
ohapieng

Figure 7: Un exemple de formulaire d'Activation dûment rempli

Onzième étape. **Cliquez** sur Finaliser pour conclure le processus de création de votre compte **RiseUp**:

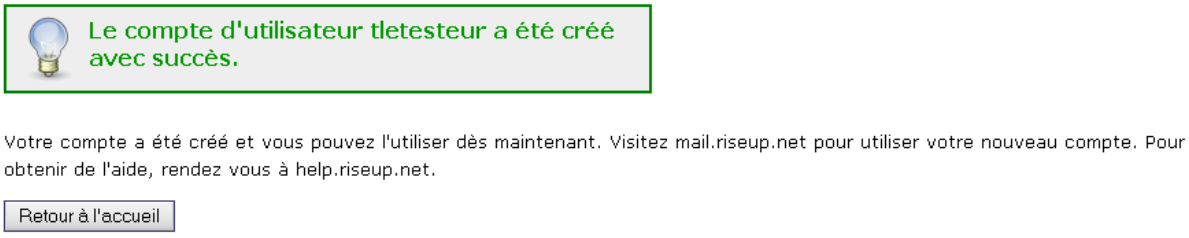

Le compte d'utilisateur tletesteur a été créé avec succès.
Votre compte a été créé et vous pouvez l'utiliser dès maintenant. Visitez mail.riseup.net pour utiliser votre nouveau compte. Pour obtenir de l'aide, rendez vous à help.riseup.net.
Retour à l'accueil

Figure 8: Un exemple de confirmation de création du compte

Douzième étape. **Cliquez** sur Suivant >> pour revenir à la *figure 2*.

Félicitations! Vous avez réussi à créer un compte de courriel **RiseUp** et vous serez automatiquement redirigé vers la *Figure 2*.

Comment vous connecter à votre compte Riseup

Sommaire des sections de cette page:

- **3.0 Comment vous connecter à votre compte RiseUp**
- **3.1 Comment utiliser le Virtual Keyboard**

3.0 Comment vous connecter à votre compte RiseUp

Pour vous connecter à votre compte **RiseUp**, suivez les étapes énumérées ci-dessous:

Première étape. **Ouvrez** la page d'accueil de **RiseUp** eMail en mode SSL **https://mail.riseup.net/** [121]

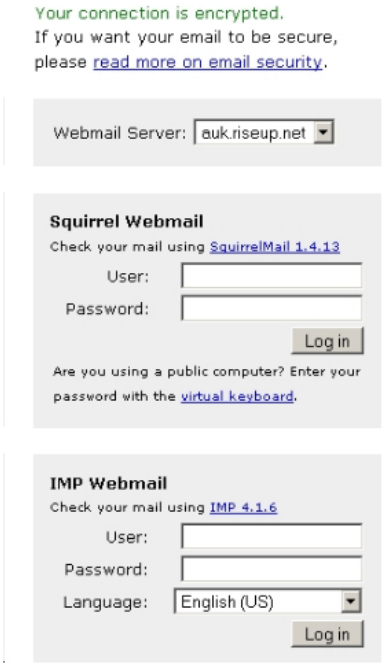


Figure 1: La page de connexion de RiseUp Mail

La page de connexion au service de courriel de **RiseUp** est séparée en deux, avec la section de *connexion* à gauche et les *Nouvelles* à droite.

Commentaire: Vous avez le choix entre deux systèmes de *webmail*. Vous pouvez utiliser l'un ou l'autre des système *webmail, mais le *webmail IMP* est mieux adapté aux interfaces qui ne sont pas en anglais.

Deuxième étape. **Saisissez** l'information appropriée dans les zones de texte *User* et *Password*, soit dans la section *Squirrelmail*, soit dans la section *IMP webmail*. N'incluez pas la formule '@riseup.net' dans la zone de texte *User*.

Étape optionnelle. **Sélectionnez** votre langue d'usage dans le menu défilant *Language*, dans la section *IMP webmail*, si nécessaire.

Troisième étape. **Cliquez** sur Log in pour afficher votre compte:

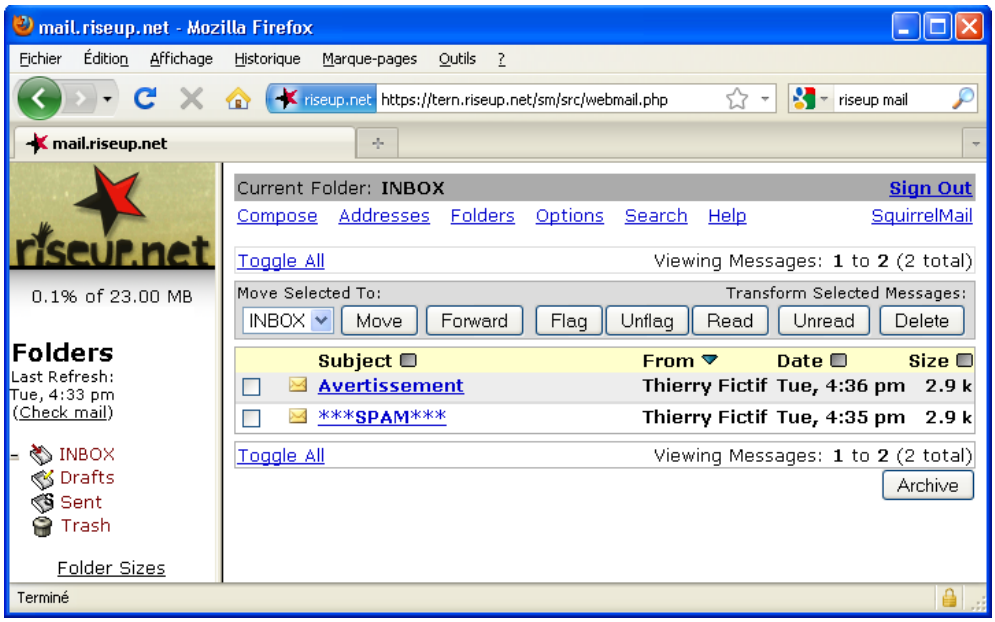


Figure 2: Un exemple de compte de courrier électronique RiseUp

Étape optionnelle: Si vous écrivez et recevez surtout des courriels dans une police de caractères non latine, vous voudrez sans doute le spécifier dans votre compte webmail. **Sélectionnez** Options dans le menu du haut pour afficher les options de *SquirrelMail*:

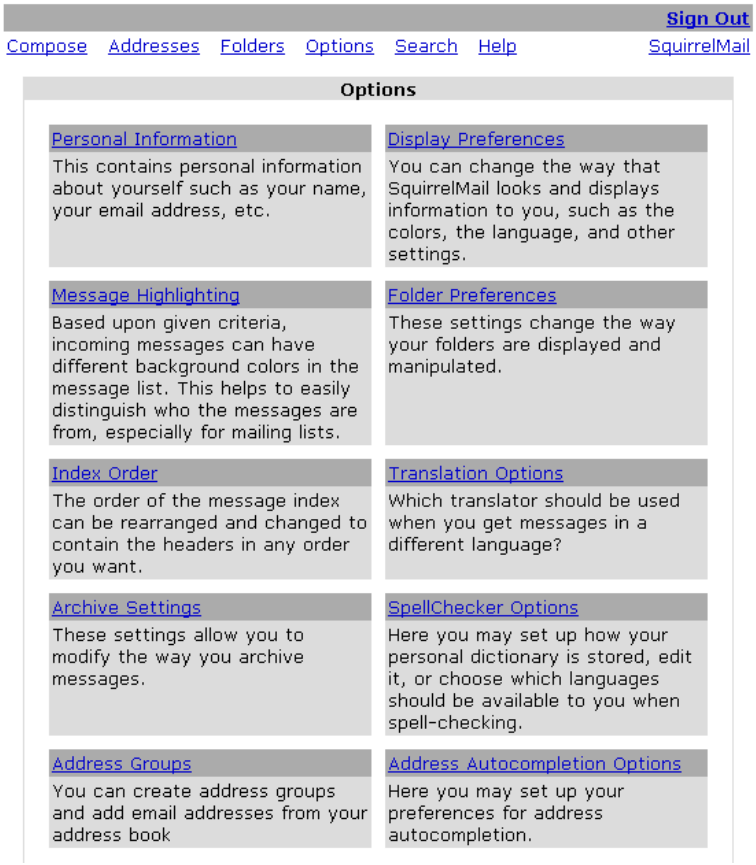

Sign Out
Compose Addresses Folders Options Search Help SquirrelMail
Options
Personal Information
This contains personal information about yourself such as your name, your email address, etc.
Display Preferences
You can change the way that SquirrelMail looks and displays information to you, such as the colors, the language, and other settings.
Message Highlighting
Based upon given criteria, incoming messages can have different background colors in the message list. This helps to easily distinguish who the messages are from, especially for mailing lists.
Folder Preferences
These settings change the way your folders are displayed and manipulated.
Index Order
The order of the message index can be rearranged and changed to contain the headers in any order you want.
Translation Options
Which translator should be used when you get messages in a different language?
Archive Settings
These settings allow you to modify the way you archive messages.
SpellChecker Options
Here you may set up how your personal dictionary is stored, edit it, or choose which languages should be available to you when spell-checking.
Address Groups
You can create address groups and add email addresses from your address book
Address Autocompletion Options
Here you may set up your preferences for address autocompletion.

Figure 3: Les options de SquirrelMail

Quatrième étape. **Sélectionnez** Display Preferences pour afficher le panneau *Options - Préférences d'affichage*, illustré ci-dessous:

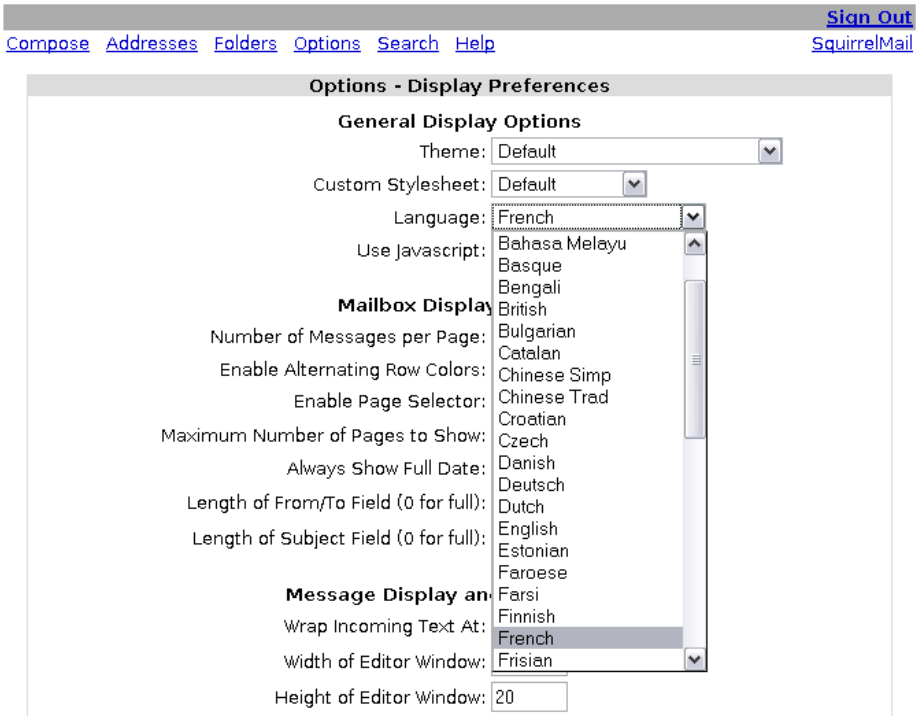


Figure 4: Le panneau Options - Préférences d'affichage de SquirrelMail

Cinquième étape. **Trouvez** le menu défilant *Language*, illustré à la *figure 4* ci-dessus, puis **sélectionnez** la langue appropriée, dans cet exemple, *Français*.

Cette option servira à déterminer l'encodage approprié à l'affichage des messages que vous enverrez et recevrez.

3.1 Comment utiliser le Clavier virtuel

Si vous utilisez un ordinateur public ou partagé (dans un café Internet, un centre communautaire ou une bibliothèque, par exemple), vous pouvez utiliser le *Clavier virtuel* (*Virtual Keyboard*) pour saisir votre mot de passe. Cette méthode vous offre une mesure de protection supplémentaire contre les *enregistreurs de frappe* (programmes *key-logger*). Les enregistreurs de frappe sont conçus pour contrôler les séquences de frappe d'un utilisateur sur un clavier physique et ainsi déduire les mots de

passe, les noms d'utilisateur et autres renseignements importants. Les claviers virtuels contournent cette vulnérabilité en permettant aux utilisateurs de saisir un mot de passe à l'aide d'une souris.

Pour utiliser le *Clavier virtuel* de **RiseUp**, suivez les étapes énumérées ci-dessous:

Première étape. **Ouvrez** la page d'accueil de **RiseUp** en mode *SSL* **https://mail.riseup.net/** [121].

Deuxième étape. **Cliquez** sur virtual keyboard pour afficher la page de connexion de **RiseUp**, tel qu'illustré ci-dessous:

Figure 5: La page de connexion de RiseUp

Troisième étape. **Cliquez** sur virtual keyboard pour afficher le *Clavier virtuel*, tel qu'illustré ci-dessous:

Figure 6: Le Clavier virtuel

Quatrième étape. À l'aide de votre souris, **cliquez** sur sur les touches qui forment votre mot de passe (ou positionnez votre curseur au dessus de chaque caractère pendant deux secondes).

Cinquième étape. **Cliquez** sur Log in pour accéder à votre compte **RiseUp**.

Comment modifier les paramètres de votre compte

Sommaire des sections de cette page:

- **4.0 Comment modifier les paramètres de votre compte**
- **4.1 La page Mes paramètres**
- **4.2 La page des paramètres du Courriel**
- **4.3 La page Invitations**

4.0 Comment modifier les paramètres de votre compte

RiseUp vous permet de modifier certains paramètres de votre compte. Vous pouvez préciser la taille de votre boîte aux lettres, changer votre nom d'utilisateur, votre adresse et votre mot de passe, ajouter des alias, etc. Vous pouvez également générer des codes d'invitation pour aider vos amis et collègues à enregistrer leur propre compte **RiseUp**.

Première étape. **Ouvrez** la page de *configuration de l'utilisateur* **RiseUp** *Account Settings*: **https://user.riseup.net/** [122]

riseup.net
home mail lists hosting help status donate
français
user.riseup.net
Nom d'utilisateur
Mot de passe
Se connecter
J'ai oublié mon mot de passe
Bienvenue au panneau de configuration de l'utilisateur riseup.net. D'ici, vous pourrez gérer les paramètres de votre compte, tel que votre mot de passe, votre nom de domaine, votre quota et vos alias. Cette interface est actuellement en construction et offrira bientôt d'autres fonctions utiles.
powered by nest
Nest where Riseup birds call home, it is where you can edit all of your your settings.
Request a new account
Créer un billet de dépannage

Figure 1: La page user.riseup.net

Deuxième étape. **Saisissez** vos détails de connexion dans les zones de texte *Nom d'utilisateur* et *Mot de passe*.

Troisième étape. **Cliquez** sur Se connecter pour afficher la fenêtre suivante:

riseup.net
home mail lists hosting help status donate
thierryfictif
Panneau de configuration de l'utilisateur %s
français
Mes paramètres
Courriel
Billets de dépannage
Mutual Aid
Invites
Shell
Logout
Page d'accueil de %s
Bienvenue au panneau de configuration de votre compte d'utilisateur. Bientôt, ce sera pour vous un endroit important où vous pourrez régler vos préférences, obtenir de l'aide et demander de nouveaux services. Actuellement, le panneau de configuration permet uniquement le réglage des préférences du compte de courriel.
Obtenir de l'aide
1. M'aider avec mon compte de courriel »
2. M'aider avec mon liste de diffusion »
Demander un nouveau service
1. Close my email account »
2. More to come soon...

Figure 2: La page de configuration du compte d'utilisateur RiseUp.net

4.1 La page Mes paramètres

La page *Mes paramètres* affiche tous les renseignements que vous avez consignés à votre compte à la section **2.1 Le formulaire d'Information sur le compte** [123].

Première étape. **Cliquez** sur Mes paramètres pour afficher la fenêtre suivante:

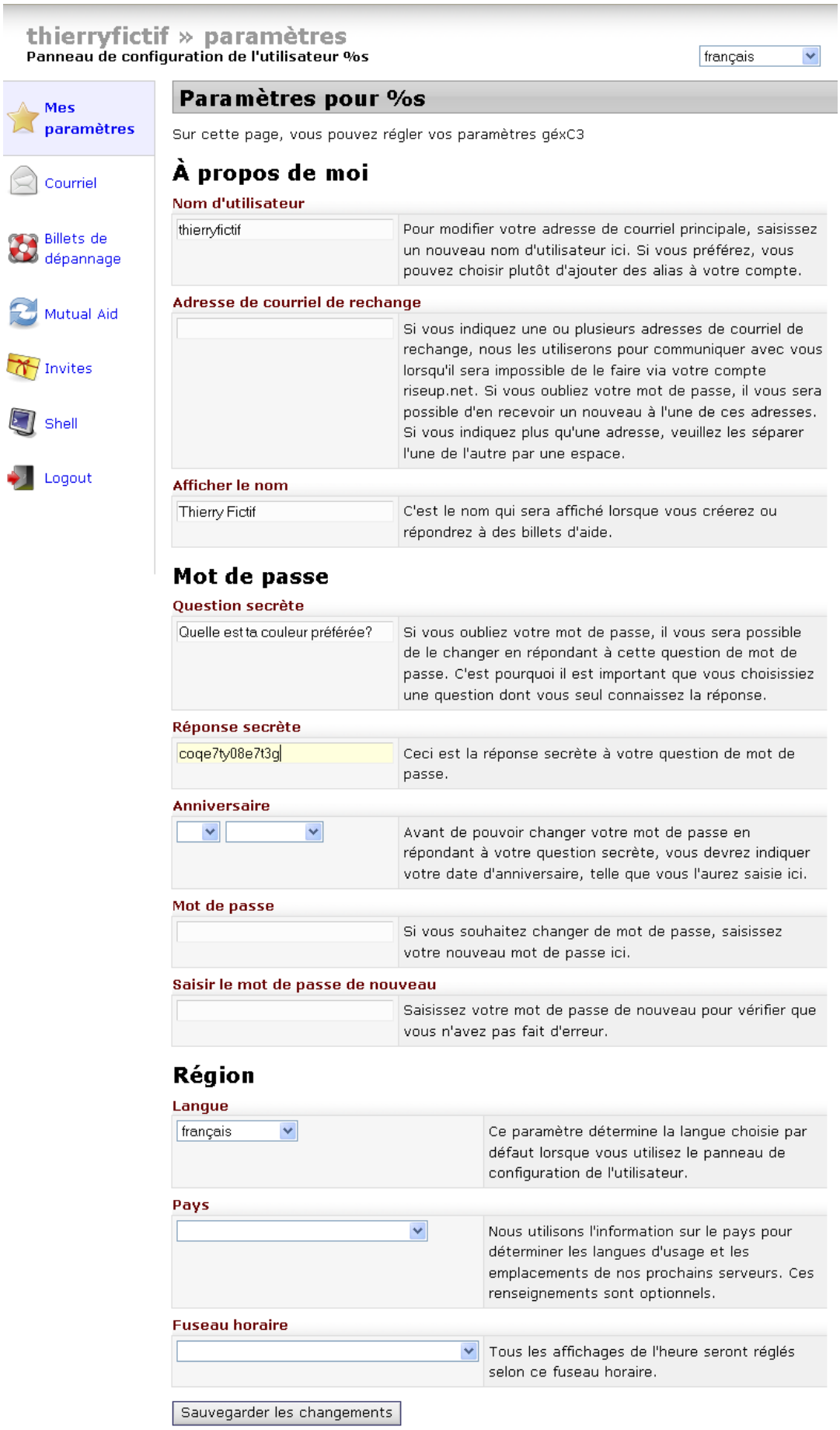

thierryfictif » paramètres
Panneau de configuration de l'utilisateur %s
français
Mes paramètres
Courriel
Billets de dépannage
Mutual Aid
Invites
Shell
Logout
Paramètres pour %s
Sur cette page, vous pouvez régler vos paramètres géxC3
À propos de moi
Nom d'utilisateur
thierryfictif
Pour modifier votre adresse de courriel principale, saisissez un nouveau nom d'utilisateur ici. Si vous préférez, vous pouvez choisir plutôt d'ajouter des alias à votre compte.
Adresse de courriel de rechange
Si vous indiquez une ou plusieurs adresses de courriel de rechange, nous les utiliserons pour communiquer avec vous lorsqu'il sera impossible de le faire via votre compte riseup.net. Si vous oubliez votre mot de passe, il vous sera possible d'en recevoir un nouveau à l'une de ces adresses. Si vous indiquez plus qu'une adresse, veuillez les séparer l'une de l'autre par une espace.
Afficher le nom
Thierry Fictif
C'est le nom qui sera affiché lorsque vous créerez ou répondrez à des billets d'aide.
Mot de passe
Question secrète
Quelle est ta couleur préférée?
Si vous oubliez votre mot de passe, il vous sera possible de le changer en répondant à cette question de mot de passe. C'est pourquoi il est important que vous choisissiez une question dont vous seul connaissez la réponse.
Réponse secrète
coqe7ty08e7t3g
Ceci est la réponse secrète à votre question de mot de passe.
Anniversaire
Avant de pouvoir changer votre mot de passe en répondant à votre question secrète, vous devrez indiquer votre date d'anniversaire, telle que vous l'aurez saisie ici.
Mot de passe
Si vous souhaitez changer de mot de passe, saisissez votre nouveau mot de passe ici.
Saisir le mot de passe de nouveau
Saisissez votre mot de passe de nouveau pour vérifier que vous n'avez pas fait d'erreur.
Région
Langue
français
Ce paramètre détermine la langue choisie par défaut lorsque vous utilisez le panneau de configuration de l'utilisateur.
Pays
Nous utilisons l'information sur le pays pour déterminer les langues d'usage et les emplacements de nos prochains serveurs. Ces renseignements sont optionnels.
Fuseau horaire
Tous les affichages de l'heure seront réglés selon ce fuseau horaire.
Sauvegarder les changements

Figure 3: La page Mes paramètres

Dans cette fenêtre, vous pouvez changer de nom d'utilisateur, ce qui modifiera également votre adresse de courrier électronique. Le nouveau nom d'utilisateur doit donc être original. C'est aussi sur cette page qu'il vous est possible de modifier d'autres paramètres du compte, tel que votre adresse de courriel de rechange, votre mot de passe, et ainsi de suite.

Première étape. **Saisissez** les nouveaux renseignements dans les zones appropriées, puis **cliquez** sur Sauvegarder les changements pour afficher le message suivant:

Figure 4: Changements sauvegardés avec succès

4.2 La page des paramètres du Courriel

La page *paramètres du Courriel* vos permet d'afficher ou de modifier les paramètres de stockage de votre courrier électronique. Vous pouvez déterminer le "quota" ou l'espace réservé à votre compte webmail sur un des serveurs de **RiseUp**.

Première étape. **Cliquez** sur

pour afficher la fenêtre suivante:

thierryfictif » courriel

Panneau de configuration de l'utilisateur %s

français

- Mes paramètres
- **Courriel**
- Billets de dépannage
- Mutual Aid
- Invites
- Shell
- Logout

Email paramètres

Ma boîte de courriel | Paramètre de gestion des pourriels | filtres-courriel

Sur cette page, vous pouvez régler vos préférences de messagerie, tel que vos quota, vos alias et vos transferts de messages.

Adresse	thierryfictif@riseup.net	Voici votre adresse de courriel. Pour toute modification, rendez vous à "Mes paramètres".
Conserver les fichiers de sauvegarde	☑	Si vous cochez cette option, nous conserverons une copie de sauvegarde de vos courriels. Si nos serveurs explosent ou si votre client de messagerie supprime tous vos courriels, vous serez en mesure de récupérer toutes vos donxC3
Quota	23 mégaoctets	Vous pouvez régler vous-même le quota de votre boîte de courriel. Cependant, n'oubliez pas que l'espace de stockage constitue notre dépense matérielle la plus importante. Si vous augmentez votre quota, veuillez également augmentez votre contribution !
Hôte du stockage	cormorant-pn.riseup.net	Ceci est le nom d'hôte Internet du serveur où vos courriels sont stockés. Veuillez éviter de faire pointer votre client IMAP ou POP directement vers votre hôte Internet.

Alias et transferts

Alias	tresbontesteur testeursur	Les alias sont des adresses de courriel supplémentaires que votre compte peut utiliser pour recevoir des courriels. Indiquez une adresse de courriel complète, à raison d'une par ligne. Pour l'instant, seulement les adresses @riseup.net sont permises.
Transférer		Indiquez une adresse de courriel où seront transférés tous les courriels expédiés à votre compte riseup.net. Tant et aussi longtemps que vous aurez un transfert configuré, vous ne recevrez aucun courriel à riseup.net.

Réparer la boîte de courriel | Restore mail from backups | Détruire la boîte de courriel

Sauvegarder les changements

Figure 5: La page des paramètres du Courriel

Deuxième étape. **Saisissez** un nombre approprié dans la zone *Quota*.

Commentaire: La taille de votre compte est limitée à un maximum de 47 Mo. Cela est considéré comme une taille suffisante pour les communications par courriel.

RiseUp n'est peut-être pas le meilleur choix si vous souhaitez utiliser un compte de courriel pour envoyer et recevoir plusieurs pièces jointes de grande taille.

Vous pouvez également créer des alias pour votre compte. Un alias est comme un surnom pour votre compte. Alors que le nom de compte principal restera inchangé, on pourra également envoyer des messages aux adresses de vos alias.

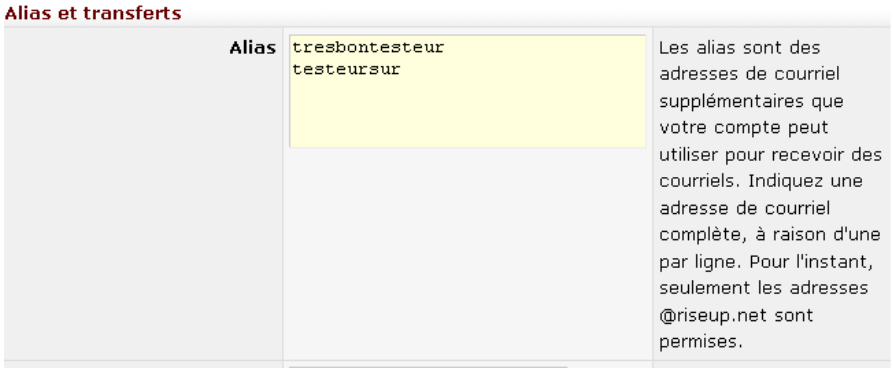

Alias et transferts
Alias
tresbontesteur
testeursur
Les alias sont des adresses de courriel supplémentaires que votre compte peut utiliser pour recevoir des courriels. Indiquez une adresse de courriel complète, à raison d'une par ligne. Pour l'instant, seulement les adresses @riseup.net sont permises.

Figure 6: La section Alias

Exemple: Le compte **thierryfictif@riseup.net** comporte maintenant deux alias. Les messages expédiés à **tresbontesteur@riseup.net** et à **testeursur@riseup.net** seront transférés au compte principal. Cela peut s'avérer pratique pour garder votre véritable adresse confidentielle.

Quatrième étape. **Cliquez** sur Sauvegarder les changements pour sauvegarder vos nouveaux alias.

4.3 La page Invitations

La page *Invitations* vous permet de générer des *codes d'invitation* qui servent à inviter vos amis et collègues à créer un compte **RiseUp**.

Important: Rappelez-vous que chaque nouveau compte exige deux codes d'invitation provenant de deux membres différents. Vous pouvez générer autant de codes que vous le souhaitez.

Première étape. **Cliquez** sur Invitations pour afficher la fenêtre suivante:

riseup.net
home mail lists hosting help status donate
thierryfictif » Invitations
Panneau de configuration de l'utilisateur %s
français
Mes paramètres
Courriel
Billets de dépannage
Mutual Aid
Invites
Shell
Logout
Invitations
Vous pouvez inviter des gens à créer des comptes riseup.net en créant des codes d'invitation. Il faut les codes d'invitation de deux utilisateurs différents pour créer un nouveau compte. AVERTISSEMENT: Si vous donnez un code d'invitation à quelqu'un que vous ne connaissez pas, nous nous réservons le droit de fermer votre compte.
Code
Expire le
Vous n'avez aucune invitation active
Créer un nouveau code d'invitation

Figure 7: La page Invitations

Deuxième étape. **Cliquez** sur Créer un nouveau code d'invitation pour générer des codes d'invitation:

Code	Expire le
uzamaloo	Feb 25 2011
niejuhai	Feb 25 2011

Imprimer les invitations | Créer un nouveau code d'invitation

Figure 8: Un exemple de code d'invitation généré automatiquement

Commentaire: Chaque code d'invitation n'est valide que pour un mois.

Troisième étape. **Cliquez** sur Imprimer les invitations pour imprimer une copie des codes d'invitation et la remettre à la personne qui souhaite

enregistrer un compte avec **RiseUp**.

Quatrième étape. **Cliquez** sur Déconnecter pour vous déconnecter de l'interface *Utilisateur*.

Faq et questions récapitulatives

5.0 Faq et questions récapitulatives

Muhindo et Salima sont ravis de constater à quel point il est facile d'utiliser **RiseUp** et sont impressionnés par l'engagement du collectif envers des valeurs sociales progressistes. Par contre, quelques questions subsistent. Heureusement leur père, Assani, est en mesure de leur donner les réponses.

***Q**: Dans quelles circonstances devrait-on utiliser **IMP** plutôt que **SquirrelMail**?*

***A**: Bonne question! En fait, il n'y a pas vraiment de différence. Si, pour une raison ou une autre, un des service webmail ne fonctionne pas ou est en cours de réparation ou de mise à jour, vous pouvez toujours utiliser l'autre service sans interruption. De plus, **IMP** offre un meilleur service pour les utilisateurs non anglophones.*

***Q**: En créant mon compte, j'ai réalisé que je ne suis pas obligé de fournir des renseignements privés.*

***A**: En effet, personne n'est obligé de le faire. Par contre, n'oubliez pas de changer vos mots de passe tous les 3 à 6 mois.*

*__Q__: Maintenant que Muhindo et moi disposons de comptes **RiseUp**, comment pouvons-nous en enregistrer un pour toi Assani?
*

***A**: Vous devez tous les deux créer un code d'invitation, puis me les envoyer.Lorsque je créerai mon propre compte, j'utiliserai vos codes d'invitation.*

Commentaire: Comme **RiseUp** dépend entièrement de dons et de la bonne volonté et du travail acharné d'une équipe de bénévoles, il n'est pas facile de faire compétition aux fournisseurs commerciaux de services de courrier électronique. Néanmoins, **RiseUp** a mis en ligne sa propre alternative (gratuite et en source ouverte) à **Facebook**, nommée **Crabgrass**. Le service présente des normes de confidentialité et de sécurité accrues et s'adresse principalement aux organismes communautaires et aux organisations non gouvernementales, ainsi qu'aux organismes de base. Pleine d'ambition et d'énergie, l'équipe de **RiseUp** espère être en mesure d'offrir ces services compétitifs et révolutionnaires dans un avenir rapproché:

- Édition collective de documents (**Etherpad**): Ce service permet à plusieurs utilisateurs d'éditer simultanément un même document.
- Proxy Internet chiffré (**openvpn**): Ce service permet de naviguer sur Internet en utilisant un serveur proxy chiffré semblable à **Tor**.
- Clavardage en temps réel (**XMPP**): Ce service permet de clavarder en temps réele et constitue l'équivalent **RiseUp** de la fonction *chat* de **Gmail** ou de la **Messagerie instantanée de Microsoft**.

5.1 Questions récapitulatives

- Quelle est la différence entre la récupération du courriel par Webmail ou à l'aide d'un client de messagerie?
- Qu'est-ce qu'un *Secure Socket Layer (SSL)* et comment cela fonctionne t-il?
- Qu'est-ce qu'un clavier virtuel, et comment cela fonctionne t-il?
- Comment peut-on ajouter un alias à un compte de courriel?
- Combien de temps un code d'invitation demeure t-il valide?

Pidgin + OTR - messagerie instantanée sécurisée

Pidgin est un client de source ouverte qui vous permet d'organiser et de gérer vos différents comptes de messagerie instantanée (MI) à l'aide d'une seule et unique interface. Le module complémentaire OTR est conçu pour sécuriser et authentifier les communications par Pidgin.

Site Internet

www.pidgin.im [124]

Configuration requise :

- Une connexion Internet

Pour installer Pidgin et OTR

- *Lisez la courte introduction des Guides pratiques [13]*
- ***Cliquez sur l'icône de Pidgin ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire,*

- Compatible avec toutes les versions de Windows

Versions utilisées pour rédiger ce guide :

- Pidgin 2.5.2 et OTR 3.2.0

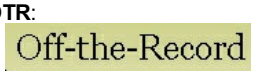
Licence :

- FLOSS (Free/libre Open Source Software)

sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- ***Installez OTR**, en utilisant la même méthode, dans le répertoire de Pigin que vous venez de créer.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

Pidgin: **OTR**:

[125]



[126]

Lecture requise :

- Livret pratique Security in-a-box, chapitre 7. Préserver la confidentialité de vos communications sur Internet [127].

Niveau : 1: Débutant, **2: Moyen**, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage : 30 minutes

Ce que vous apportera l'utilisation de cet outil :

- La capacité d'organiser et de gérer certains des services de messagerie instantanée les plus connus à l'aide d'un seul programme;
- La possibilité de mener des séances de clavardage (chat) privées et sécurisées.

1.1 À propos de cet outil

Pidgin est un client de source ouverte qui vous permet d'organiser et de gérer vos différents comptes de messagerie instantanée (MI) avec une seule et unique interface. Avant de commencer à utiliser Pidgin, vous devez disposer d'au moins un compte de MI. Par exemple, si vous possédez un compte de courriel *Gmail* ou *Yahoo*, vous pouvez utiliser les services de MI offerts par ces compagnies avec Pidgin. Utilisez les détails de connexion associés à ces comptes pour y accéder via Pidgin.

Commentaire : Tous les utilisateurs sont fortement encouragés à en apprendre le plus possible sur les politiques de leurs fournisseurs de service de MI en matière de confidentialité et de sécurité.

Pidgin est compatible avec les services de MI suivants : AIM [128]; Google Talk [129]; ICQ [130]; IRC [131]; MSN [132]; QQ [133]; Yahoo! [134] ainsi que tous les clients de MI utilisant le protocole XMPP.

Pidgin ne permet pas la communication entre différents services de MI. Par exemple, si vous utilisez Pidgin pour accéder à votre compte *Google Talk*, il ne vous sera pas possible de clavarder avec un ami qui utilise plutôt Pidgin avec son compte *Yahoo*. Par contre, si vous utilisez Pidgin pour vous connecter à plusieurs comptes, alors vous pouvez vous servir du programme pour clavarder avec ceux de vos amis qui disposent d'au moins un de ces services. Il est conseillé d'utiliser Pidgin pour tous vos besoins en matière de messagerie instantanée, puisque ce programme offre plus de sécurité que la plupart des options qui existent et ne vient pas par défaut avec des logiciels publicitaires ou espions superflus.

La **messagerie OTR (Off-the-Record)** est un module complémentaire, conçu tout spécialement pour Pidgin, qui vous permet de clavarder en privé et vous offre les fonctions suivantes:

- *Chiffrement* : Personne d'autre que vous ne peut lire vos communications instantanées.
- *Authentification* : Vous êtes assuré que votre correspondant est bel et bien la personne que vous croyez.
- *Possibilité de démenti (*deniability*)* : Après votre conversation, il est impossible de retracer les messages jusqu'à vous ou jusqu'à votre correspondant.
- *Perfect Forward Secrecy* : Si vous perdez la maîtrise de vos clés privées, vos conversations préalables ne sont pas compromises.

Commentaire : Vous devez installer le programme Pidgin avant d'installer **Pidgin OTR**.

Comment utiliser Pidgin

Avant de commencer à utiliser **Pidgin**, vous devez disposer d'un compte avec l'un ou l'autre des fournisseurs de service listés ci-dessus. Vous devez saisir dans Pidgin vos renseignements de connexion à la MI.

Commentaire : Si vous ne disposez pas déjà d'un compte avec l'un ou l'autre des fournisseurs de service listés ci-dessus et souhaitez obtenir de l'aide pour en créer un, veuillez vous référer à la section **4.1 Comment créer un compte Google Talk** [135].

2.1 Comment créer un compte Pidgin

Première étape. **Sélectionnez : Démarrer > Tous les programmes > Pidgin** pour lancer Pidgin.

Liste de contacts
Contacts Comptes Outils Aide
Bienvenue dans Pidgin !
Vous n'avez aucun compte actif. Activez vos comptes de messagerie depuis la fenêtre Comptes dans le menu Comptes⇨Gérer. Une fois les comptes activés, vous pourrez vous connecter, changer votre état et discuter avec vos contacts.

Figure 1 : L'écran de bienvenue à la liste de contacts de Pidgin

Deuxième étape. **Sélectionnez : Comptes > Gérer** pour activer la fenêtre *Comptes* illustrée ci-dessous :

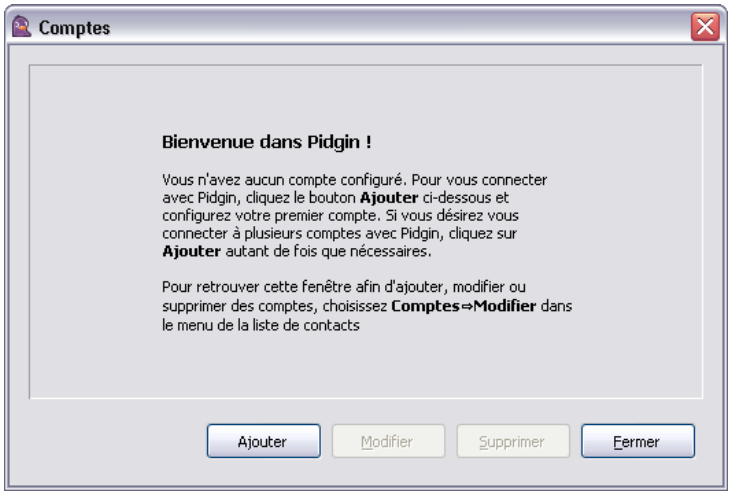

Comptes
Bienvenue dans Pidgin !
Vous n'avez aucun compte configuré. Pour vous connecter avec Pidgin, cliquez le bouton Ajouter ci-dessous et configurez votre premier compte. Si vous désirez vous connecter à plusieurs comptes avec Pidgin, cliquez sur Ajouter autant de fois que nécessaires.
Pour retrouver cette fenêtre afin d'ajouter, modifier ou supprimer des comptes, choisissez Comptes⇨Modifier dans le menu de la liste de contacts
Ajouter
Modifier
Supprimer
Fermer

Figure 2 : La fenêtre Comptes

Troisième étape. **Cliquez** sur: pour activer la fenêtre *Ajouter un compte* illustrée ci-dessous :

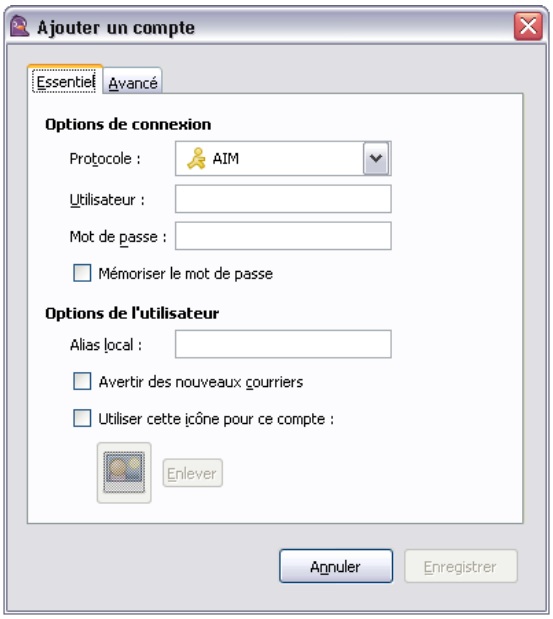


Figure 3 : La fenêtre Ajouter un compte affichant les onglets Essentiel et Avancé

Quatrième étape. **Cliquez** sur le menu défilant *Protocole* pour afficher la liste des fournisseurs de messagerie instantanée compatibles :

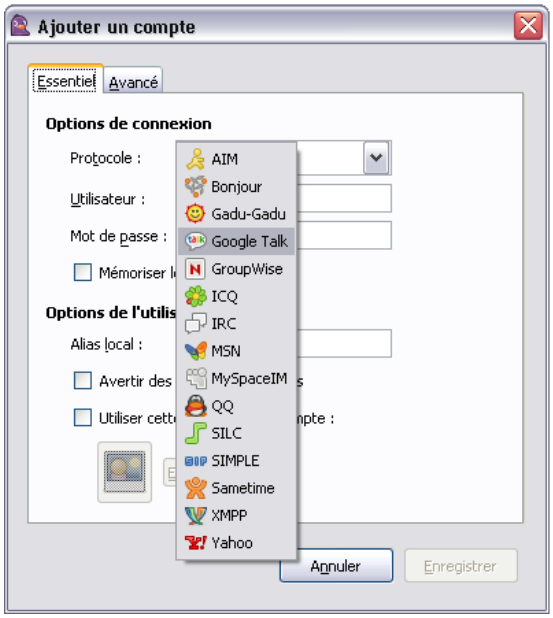


Figure 4 : La fenêtre Ajouter un compte affichant le menu défilant Protocole

Cinquième étape. **Sélectionnez** le protocole qui correspond à votre compte.

Commentaire : Certains fournisseurs de service de MI affichent leurs zones de texte particulières, que vous devez remplir. D'autres remplissent les zones de texte automatiquement (par exemple, si vous sélectionnez *Google Talk*, les zones de texte *Domaine* et *Ressource* sont déjà remplies pour vous). Cependant, tous les services exigent que vous saisissiez un nom d'utilisateur, un Alias local et un mot de passe.

Sixième étape. Dans la zone de texte *Utilisateur*, **saisissez** votre adresse de courriel, (par exemple, thierry.letesteur@gmail.com [136])

Septième étape. Dans la zone de texte *Mot de passe* , **saisissez** le mot de passe associé à ce compte.

Huitième étape. Dans la zone de texte *Alias local*, **saisissez** un surnom par lequel vous souhaitez être identifié. (Cette zone est optionnelle.)

Important : Cochez l'option *Mémoriser le mot de passe* si vous souhaitez que Pidgin mémorise votre mot de passe. Par contre, pour maximiser la sécurité et la confidentialité, il est souhaitable de laisser cette option décochée. Ainsi, Pidgin vous demandera de saisir votre mot de passe chaque fois que vous vous connecterez. De cette manière, personne ne sera en mesure de se connecter en usurpant votre identité si vous vous éloignez de votre ordinateur pour une longue période. Aussi, n'oubliez jamais de quitter Pidgin lorsque vous avez fini une séance de clavardage!

Une fenêtre *Ajouter un compte* dûment remplie devrait ressembler à ceci :

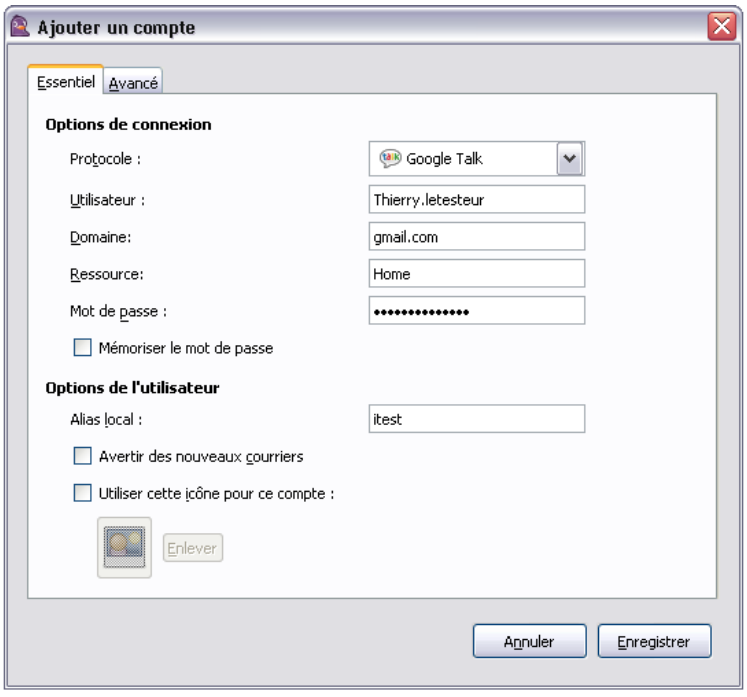


Figure 5 : Exemple de formulaire Ajouter un compte, dûment rempli

Conseil : Les clients *Google Talk*, *IRC*, *SILC* et *XMPP* sont facilement configurables pour exiger une connexion chiffrée. Veuillez pour cela consulter la section **4.2 Comment ouvrir une connexion sécurisée** [135].

Neuvième étape . **Cliquez** sur :

pour achever le processus d'ajout de compte. Cela activera simultanément la fenêtre *Comptes* et la fenêtre *Liste de contacts*, toutes deux mises à jours :

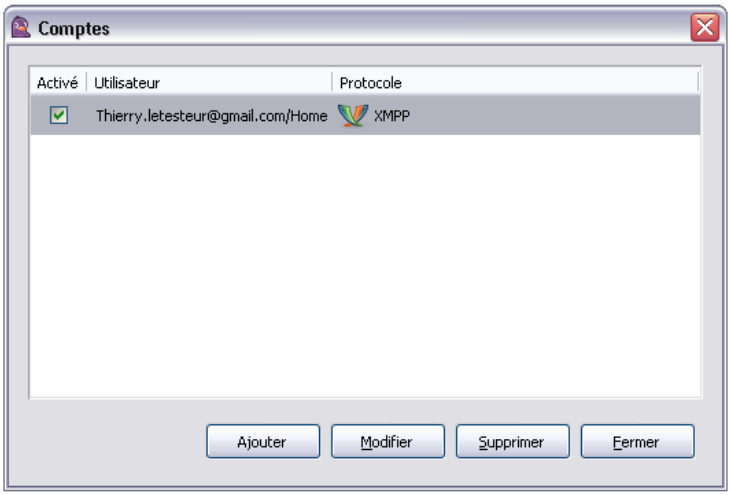


Figure 6 : La fenêtre Comptes mise à jour

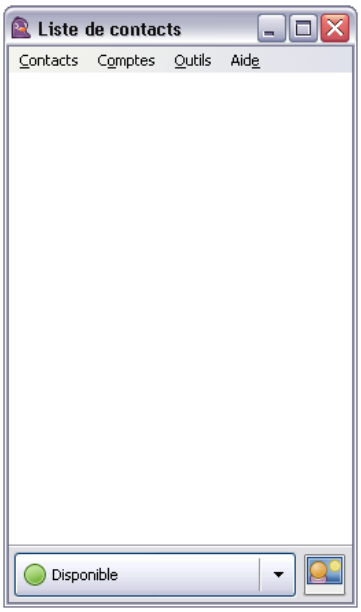


Figure 7 : La fenêtre Liste de contacts en mode actif

Après avoir complété ces étapes, vous êtes prêt à ajouter des détails personnels de MI pour chacun de vos contacts.

2.2 Comment ajouter un contact

Première étape. **Sélectionnez : Contacts > + Ajouter un contact** comme suit :

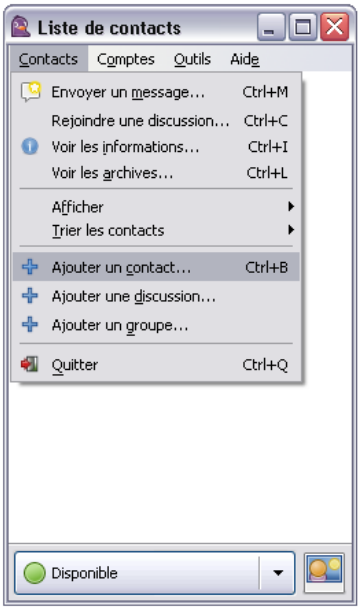


Figure 8 : La liste de contacts affichant le menu Contacts

Cette action activera la fenêtre suivante :

Figure 9 : La fenêtre Ajouter le contact

Deuxième étape. **Sélectionnez** votre compte, celui qui correspond au service de messagerie de votre nouveau "contact".

Commentaire : Il est essentiel que vous et votre contact utilisiez le même service de messagerie, et ce, même si cette personne n'utilise pas Pidgin. Par exemple, si vous avez seulement ajouté un compte *Google Talk* dans Pidgin, vous ne pourrez pas ajouter un contact qui n'utilise que *MSN* ou *Yahoo*. Cependant, vous pouvez enregistrer et utiliser simultanément plusieurs comptes dans Pidgin, ce qui vous permet de clavarder avec un contact via Google Talk et avec un autre via Yahoo ou MSN.

Troisième étape. Dans la zone de texte *Nom d'utilisateur du contact*, **saisissez** l'adresse de courriel de votre contact. (Rappelez-vous : dans Pidgin, le terme "Nom d'utilisateur" réfère généralement à une adresse de courriel.)

Quatrième étape. Dans la zone de texte *Alias*, **saisissez** un mot de passe correspondant à votre nouveau contact.

Cinquième étape. **Cliquez** sur :

Commentaire : Après avoir ajouté un contact, un message sera envoyé automatiquement à ce dernier pour lui demander une approbation ou une autorisation, selon votre requête.

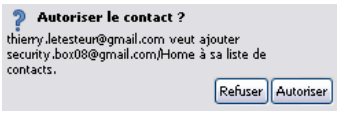


Figure 10 : La boîte de dialogue Autoriser le contact

Après que votre contact ait autorisé la requête, il ou elle devrait suivre la même procédure pour solliciter votre propre compte.

Figure 11 : La fenêtre Ajouter le contact affichant les détails du contact

Vous recevrez une requête d'autorisation comme celle-ci :

Figure 12 : La fenêtre Ajouter le contact

Sixième étape. **Cliquez** sur le bouton *Autoriser* et votre nouveau contact apparaîtra alors dans votre *Liste de contacts*, comme suit :

Figure 13 : La liste de contacts affichant un contact nouvellement ajouté

2.3 Comment clavarder avec votre contact

Première étape. **Cliquez à droite** sur le nom de votre contact pour activer ce menu défilant :

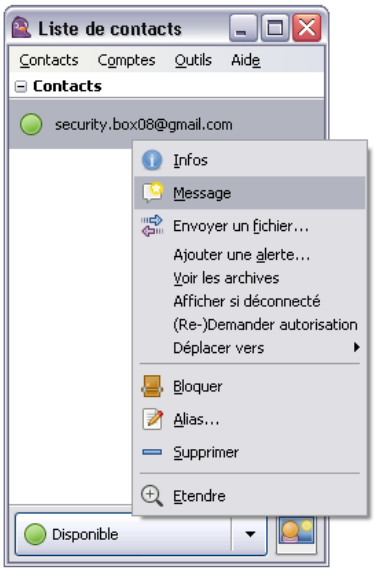


Figure 14 : Le menu des tâches de la liste de Contacts

Deuxième étape. **Sélectionnez** *Message* dans le menu défilant pour activer une fenêtre de clavardage :

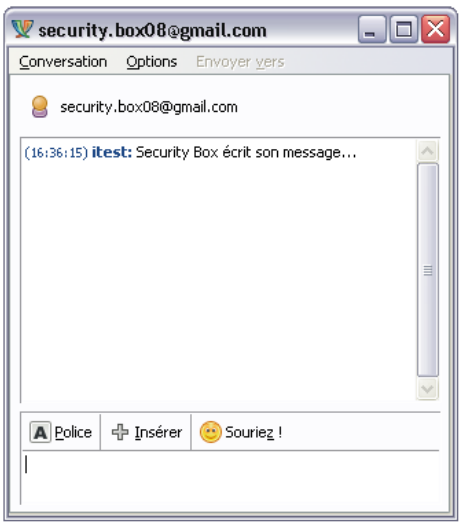


Figure 15 : Une fenêtre de clavardage typique dans Pidgin

Vous êtes désormais fin prêt à clavarder avec votre contact en utilisant Pidgin. Cependant, il vous faut encore suivre quelques étapes pour vous assurer que vos séances de clavardage soient confidentielles et sécurisées.

Comment sécuriser vos séances de clavardage OTR

Les deux parties souhaitant communiquer ensemble doivent installer et configurer le module complémentaire OTR avant d'être en mesure de mener des séances de clavardage sécurisées. Pidgin reconnaît automatiquement si les deux parties ont installé et configuré le module OTR. Si vous sollicitez une conversation confidentielle avec un contact qui n'a pas encore installé OTR, un message sera envoyé à cette personne pour lui expliquer comment obtenir le module.

3.1 Comment activer le module complémentaire Pidgin-OTR

L'activation du module **Pidgin-OTR** est la première étape à suivre afin de mener des séances de clavardage confidentielles et sécurisées. Pour ce faire, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez : Outils > Plugins** dans la fenêtre *Liste de contacts* de Pidgin, comme suit :

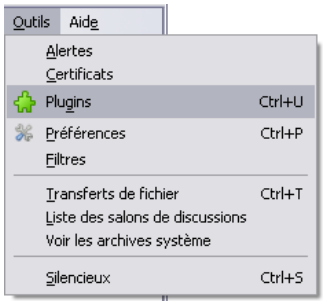


Figure 16 : Le menu Outils avec Plugins sélectionné

Cela activera la fenêtre *Plugins* illustrée ci-dessous :

Deuxième étape. **Faites défiler** jusqu'à l'option *Messagerie confidentielle Off-the-Record*, puis **cochez-la** pour activer cette fonction.

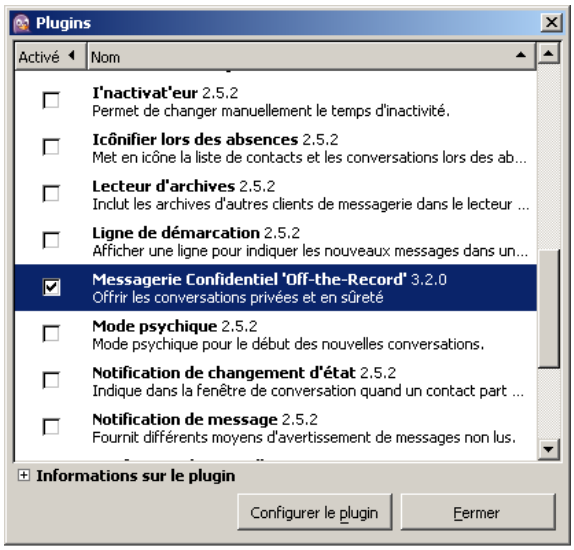
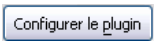

Plugins
Activé
Nom
I'nactivat'eur 2.5.2
Permet de changer manuellement le temps d'inactivité.
Icônifier lors des absences 2.5.2
Met en icône la liste de contacts et les conversations lors des ab...
Lecteur d'archives 2.5.2
Inclut les archives d'autres clients de messagerie dans le lecteur ...
Ligne de démarcation 2.5.2
Afficher une ligne pour indiquer les nouveaux messages dans un...
Messagerie Confidentiel 'Off-the-Record' 3.2.0
Offrir les conversations privées et en sûreté
Mode psychique 2.5.2
Mode psychique pour le début des nouvelles conversations.
Notification de changement d'état 2.5.2
Indique dans la fenêtre de conversation quand un contact part ...
Notification de message 2.5.2
Fournit différents moyens d'avertissement de messages non lus.
Informations sur le plugin
Configurer le plugin
Fermer

Figure 17 : La fenêtre Plugins de Pidgin avec l'option Messagerie confidentielle Off-the-Record sélectionnée

Troisième étape. **Cliquez sur** :  pour commencer à configurer l'écran *Messagerie confidentielle Off-the-Record*.

3.2 Comment générer une clé de chiffrement

Les séances de clavardage confidentielles avec Pidgin ne sont possibles qu'en générant une *clé privée* pour le compte pertinent. La fenêtre de configuration *Off-the-Record* comporte deux onglets : *Configuration* et *Empreintes connues*. L'onglet *Configuration* sert à générer une clé pour chacun de vos comptes et à régler certaines options particulières à OTR. L'onglet *Empreintes connues* contient les clés de vos contacts. Vous devez disposer d'une clé pour chaque contact avec qui vous souhaitez clavarder en mode confidentiel.

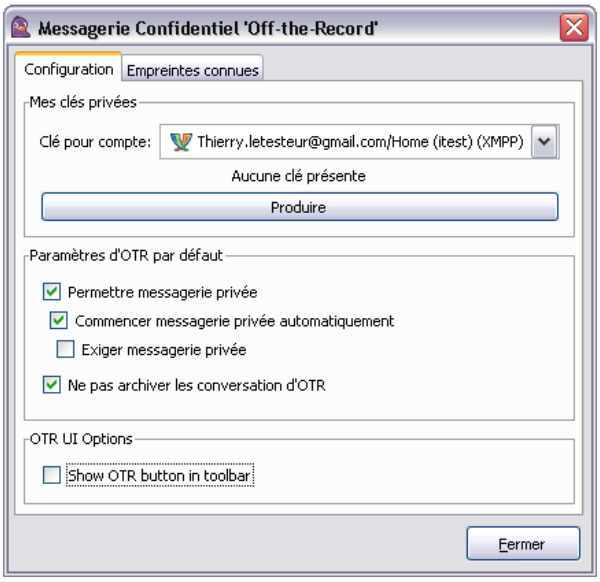


Figure 18 : L'écran Messagerie confidentielle Off-the-Record affichant l'onglet Configuration

Première étape. Pour optimiser la confidentialité de vos communications, **cochez** les options *Permettre messagerie privée*, *Commencer messagerie privée automatiquement* et *Ne pas archiver les conversations OTR* dans l'onglet *Configuration* illustré ci-dessus.

Deuxième étape. **Cliquez** sur :

pour générer votre clé. Peu de temps après, une fenêtre apparaît pour vous aviser que la clé privée a bel et bien été générée :

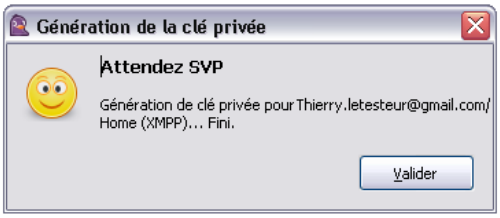

Génération de la clé privée
Attendez SVP
Génération de clé privée pour Thierry.letesteur@gmail.com/Home (XMPP)... Fini.
Valider

Figure 19 : La fenêtre Génération de la clé privée

Votre contact devra suivre les mêmes étapes sur son ordinateur.

Important : Vous venez de créer une clé privée pour votre compte. Cette clé sera utilisée pour chiffrer vos conversations de telle sorte que personne d'autre ne pourra les lire, même si quelqu'un arrive à s'interposer entre vous et vos contacts. L'empreinte est une longue séquence de lettres et de chiffres utilisés pour identifier la clé d'un compte. L'empreinte devrait ressembler à ceci :

L'empreinte : 55A3638C 5DCF5BB8 0C7A2815 70DA5122 06507354

Pidgin sauvegarde et vérifie automatiquement votre empreinte et celles de vos contacts pour que vous n'ayez pas à les mémoriser.

3.3 Comment authentifier une conversation confidentielle

Il n'y a que trois étapes faciles à suivre pour assurer la confidentialité et la sécurité de vos conversations.

- La **première étape**, que vous venez d'achever à la section **3.2 Comment générer un clé de chiffrement**, consistait à créer une clé privée pour votre compte.
- La **deuxième étape** est celle où vous et votre contact faites la requête d'une conversation sécurisée.
- La **troisième étape** sert à vérifier que votre contact est *bel et bien* la personne avec qui vous souhaitez clavarder. Cette procédure de confirmation de l'identité d'une personne s'appelle *authentification* dans Pidgin.

3.3.1 La deuxième étape

Première étape. **Double-cliquez** sur le compte d'un de vos contact en ligne pour entamer une nouvelle conversation. Si vous avez tous les deux installé et correctement configuré le module OTR, vous remarquerez qu'un nouvel icône *OTR* est apparu au bas de la fenêtre de clavardage.

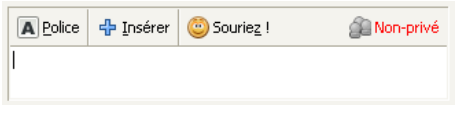
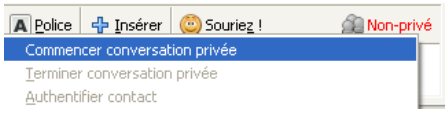


Figure 20 : Une fenêtre de clavardage de Pidgin affichant l'icône OTR

Deuxième étape. **Cliquez** sur :



Votre fenêtre de clavardage affichera le message suivant :

Création d'une conversation privée avec utilisateur@exemple

utilisateur@exemple n'a pas encore été authentifié. Vous devriez authentifier votre contact.

Une conversation non-vérifiée avec utilisateur@exemple a commencé.

Et le bouton OTR sera modifié comme suit :

Cela signifie que vous pouvez désormais entreprendre une conversation chiffrée avec votre contact. Cependant, cette conversation n'est pas vérifiée. Votre contact pourrait en fait être quelqu'un d'autre assis devant le même ordinateur, se faisant passer pour votre vrai contact. Vous devrez donc, à cette étape, partager un code secret (entendu d'avance entre vous) pour vérifier mutuellement vos identités.

3.3.2 La troisième étape

Afin d'authentifier votre contact dans Pidgin, vous devrez utiliser l'une des deux méthodes détaillées ci-dessous. Vous pouvez vous identifier mutuellement en employant un code secret ou une procédure de question et réponse.

Utiliser la méthode par code secret

Vous pouvez vous entendre sur un code secret à l'avance, soit lors d'une rencontre en personne ou en utilisant un autre moyen de communication (comme le téléphone, le téléphone Internet Skype, ou un message texte par téléphone cellulaire). Lorsque vous saisissez le même code secret chacun de votre côté, votre séance sera vérifiée (authentifiée).

Première étape. **Cliquez à droite** sur le bouton *OTR* dans la fenêtre de clavardage , puis **sélectionnez** *Authentifier contact*, comme suit :

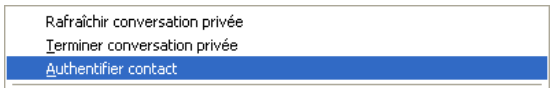


Figure 21 : Le menu OTR avec l'option Authentifier contact sélectionnée

Une fenêtre s'ouvrira vous demandant de choisir l'une ou l'autre des méthodes d'authentification.

Deuxième étape. Dans le menu défilant **sélectionnez** l'option *Shared Secret*.

Authenticate Buddy
Authentifier security.box08@gmail.com
Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.
How would you like to authenticate your buddy?
Question and answer
Question and answer
Shared secret
Manual fingerprint verification
Enter question here:
Enter secret answer here (case sensitive):
Aide
Annuler
Authenticate

Figure 22 : La fenêtre Authentifier contact

Troisième étape étape. Saisissez le code secret désiré (sensible à la casse) puis **cliquez** sur le bouton
.

Authenticate Buddy
Authentifier security.box08@gmail.com
Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.
How would you like to authenticate your buddy?
Shared secret
Pour l'authentification, choisissez un code secret connu seulement par vous et votre contact. Entrez ce secret, puis attendez que votre contact l'ait aussi entrer. Si vos secrets ne sont pas identiques, vous pourriez être en conversation avec un imposteur.
Enter secret here:
pommes
Aide
Annuler
Authenticate

Figure 23 : La fenêtre Shared Secret

De son côté, votre contact verra la même fenêtre et devra saisir le même code secret. Si les deux codes correspondent, votre séance sera authentifiée.

Lorsque la séance sera authentifiée, le bouton *OTR* ressemblera à ceci . Votre séance de clavardage est maintenant sécurisée et vous êtes assuré que la personne avec qui vous clavardez est bel et bien la personne que vous croyez.

Utiliser la méthode par question et réponse

Première étape. **Cliquez à droite** sur le bouton *OTR* dans la fenêtre de clavardage, puis **sélectionnez** *Authentifier contact*, comme suit :

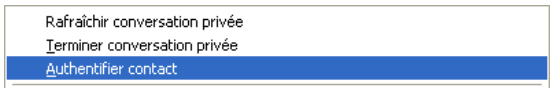


Figure 24 : Le menu OTR avec l'option Authentifier contact sélectionnée

Une fenêtre s'ouvrira vous demandant de choisir l'une ou l'autre des méthodes d'authentification.

Deuxième étape. Dans le menu défilant **sélectionnez** l'option *Question and answer*.

Authenticate Buddy
Authentifier security.box08@gmail.com
Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.
How would you like to authenticate your buddy?
Question and answer
Question and answer
Shared secret
Manual fingerprint verification
Enter question here:
Enter secret answer here (case sensitive):
Aide
Annuler
Authenticate

Figure 25 : La fenêtre Authentifier contact

Troisième étape étape. **Saisissez** une question et une réponse dans les zones de texte appropriées. La question sera acheminée à votre contact. Si vos réponses correspondent, l'authentification sera réussie.

Authenticate Buddy
Authentifier security.box08@gmail.com
Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.
How would you like to authenticate your buddy?
Question and answer
To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.
Enter question here:
Dans quelle ville nous sommes-nous rencontrés?
Enter secret answer here (case sensitive):
Dakar
Aide
Annuler
Authenticate

Figure 26 : La fenêtre Question and Answer

Lorsque la séance sera authentifiée, le bouton *OTR* ressemblera à ceci

. Votre séance de clavardage est maintenant sécurisée et vous êtes assuré que la personne avec qui vous clavardez est bel et bien la personne que vous croyez.

Félicitations! Vous pouvez maintenant clavarder en tout confidentialité. La prochaine fois que votre contact et vous voudrez clavarder (en utilisant les mêmes ordinateurs), vous pourrez sauter les étapes 1 et 2 décrites ci-dessus. Vous n'aurez qu'à demander une connexion sécurisée et votre contact n'aura qu'à l'accepter.

Remarquez que lorsque vous **Sélectionnez : Liste de contacts > Outils > Plugins > Messagerie confidentielle Off-The-Record > Configurer le plugin**, l'onglet *Empreintes connues* affiche désormais le compte de votre contact et un message indiquant que son identité a été vérifiée.

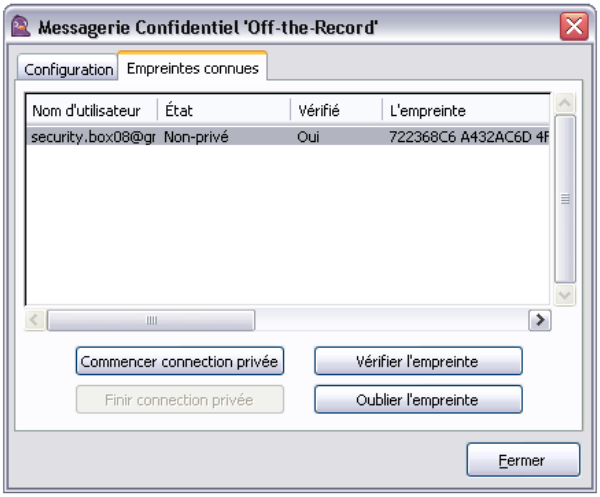


Figure 27 : L'écran de Messagerie confidentielle Off-the-Record affichant l'onglet Empreintes connues

Comment créer un compte Google Talk

4.1 Comment créer un compte Google Talk

Pour créer un compte Google Talk, suivez les étapes énumérées ci-dessous :

Première étape. **Ouvrez** votre navigateur Web et rendez-vous à la page Créer un compte Google.

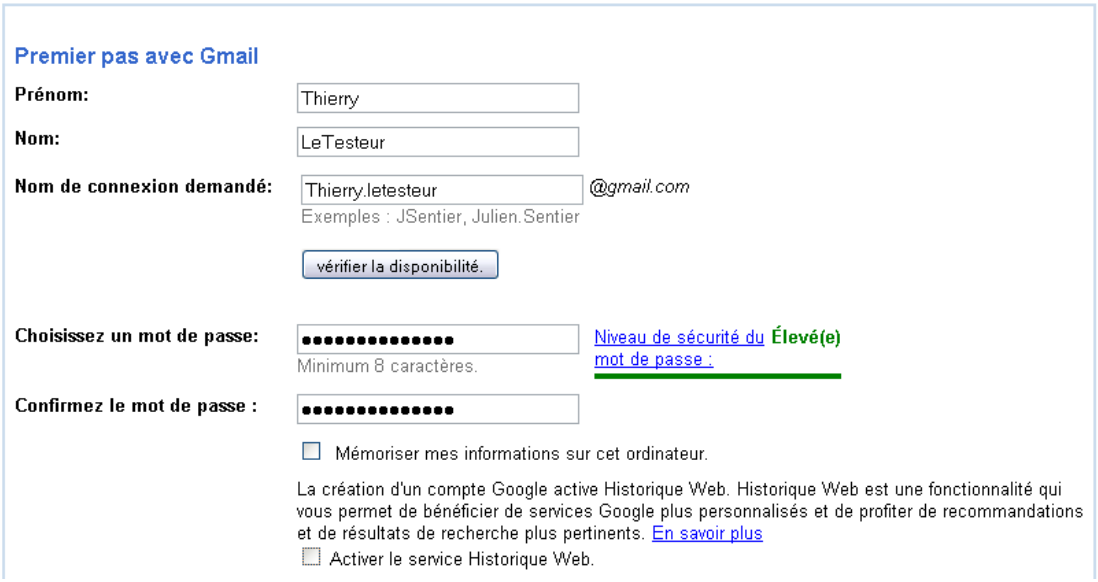

Premier pas avec Gmail
Prénom:
Thierry
Nom:
LeTesteur
Nom de connexion demandé:
Thierry.letesteur
@gmail.com
Exemples : JSentier, Julien.Sentier
vérifier la disponibilité.
Choisissez un mot de passe:
Minimum 8 caractères.
Niveau de sécurité du mot de passe : Élevé(e)
Confirmez le mot de passe :
Mémoriser mes informations sur cet ordinateur.
La création d'un compte Google active Historique Web. Historique Web est une fonctionnalité qui vous permet de bénéficier de services Google plus personnalisés et de profiter de recommandations et de résultats de recherche plus pertinents. En savoir plus
Activer le service Historique Web.

Figure 28 : La page d'enregistrement d'un nouveau compte

Deuxième étape. **Saisissez** les renseignements nécessaires.

Commentaire : Dans la zone de texte *Nom d'utilisateur souhaité :* saisissez un nom pour votre compte d'utilisateur/adresse de courriel. Pour des raisons de confidentialité et de sécurité, votre nom d'utilisateur ne devrait pas correspondre, idéalement, à vos prénom et nom de famille.

Troisième étape. **Cliquez** sur le bouton *Vérifier la disponibilité* pour vérifier si le nom que vous souhaitez est disponible. Si ce n'est pas le cas, vous devrez peut-être trouver quelque chose d'un peu plus original!

Quatrième étape. **Cliquez** sur pour accepter et créer votre compte Google Talk, après avoir rempli les zones de texte obligatoires.

4.2 Comment ouvrir une connexion sécurisée

Les utilisateurs enregistrés qui utilisent Pidgin avec un compte *Google Talk*, *IRC*, *SILC* ou un service compatible *XMPP*, peuvent configurer Pidgin pour utiliser une connexion sécurisée, généralement connue sous l'appellation *Secure Socket Layer* (*SSL*), ou *Transport Layer Security* (*TLS*).

Dans l'onglet *Essentiel* de l'écran *Modification du compte* :

Première étape. **Sélectionnez** votre fournisseur de messagerie instantanée, saisissez les renseignements nécessaires, puis **cliquez** sur l'onglet *Avancé*.

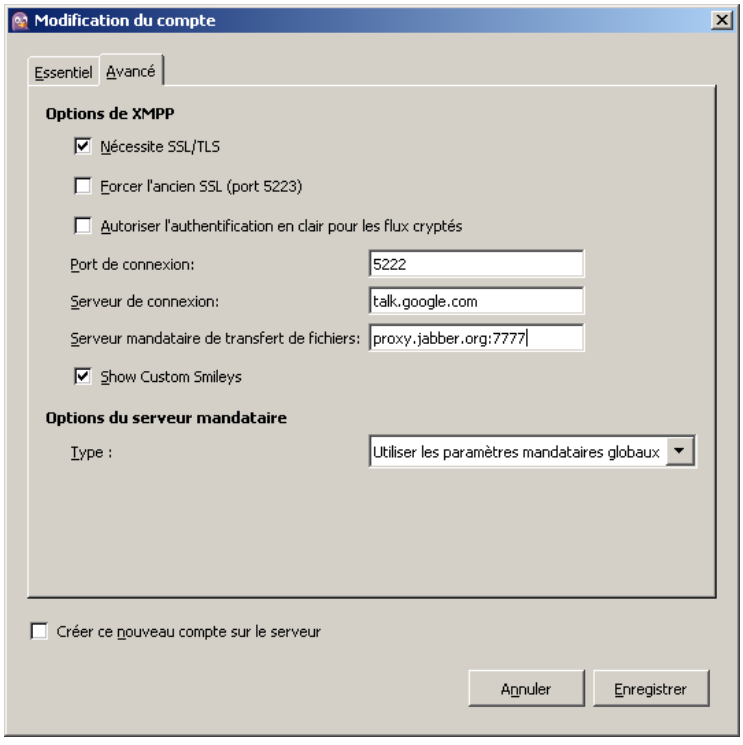


Figure 29 : L'écran Modification du compte affichant l'onglet Avancé

Deuxième étape. **Cochez** l'option *Nécessite SSL/TLS* afin d'activer automatiquement un canal sécurisé pour votre séance de messagerie instantanée.

Faq et questions récapitulatives

Q. : *J'ai éteint **Pidgin** hier soir. Aujourd'hui, quand j'ai relancé le programme, je ne trouvais plus aucun de mes contacts, même si je savais qu'ils étaient en ligne à ce moment.*

R. : *Cela se produit parfois si ton compte n'a pas été fermé correctement (la connexion à Internet a été coupée ou l'ordinateur a planté). Tu dois réactiver ton compte. Pour ce faire, **Sélectionne : Comptes > menu ajouter/modifier** et **coche** la case qui se trouve à côté de ton compte.*

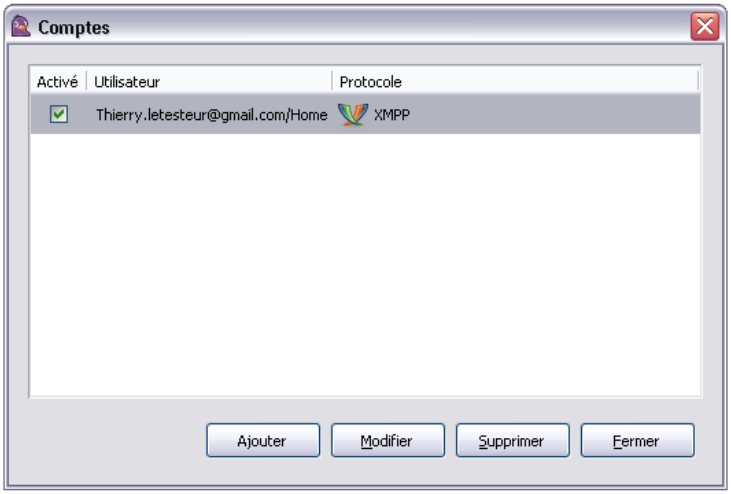


Figure 30 : La fenêtre Comptes avec votre compte réactivé

Q. : *Nikolai, est-ce que je peux utiliser Pidgin-OTR pour clavarder avec des amis dans MSN et Yahoo?*

R. : *Très bonne question, Elena. Même si Pidgin-OTR est compatible avec bon nombre de services de messagerie et de clavardage, toi et ton contact devez utiliser le même fournisseur de service pour lancer une séance de MI. Vous devez tous deux utiliser un compte MSN ou un compte Google Talk, par exemple. Cependant, dans Pidgin tu peux peux être enregistrée et connectée avec plusieurs comptes de MI simultanément. C'est l'avantage principal d'un client de MI multi-protocole.*

Q. : *Qu'arriverait-il si je devais accéder à mon compte Pidgin-OTR depuis un autre ordinateur?*

R. : *Il te faudrait générer une nouvelle clé privée pour utiliser ton compte de MI sur cet ordinateur. Tu peux entamer une conversation avec ton contact en utilisant cette nouvelle clé, mais tu devras authentifier ta séance de nouveau.*

Q. : *Qu'advient-il si j'oublie mon mot de passe pour mon compte de MI? Ou si quelqu'un le vole? Cette personne aura-t-elle accès à mes conversations passées et futures?*

R. : *C'est une question très importante. Premièrement, si tu oublies ton mot de passe d'enregistrement, tu devras créer un nouveau compte de MI. Ensuite, tu devras aviser ton contact de la création de ce nouveau compte par téléphone, Skype, téléphonie Internet, ou courriel sécurisé. Finalement, tu devrais créer une nouvelle séance authentifiée avec ton contact. Si, par ailleurs, une personne te vole ton mot de passe de MI, cette personne pourrait essayer de se faire passer pour toi en utilisant Pidgin. Heureusement, elle ne pourrait pas authentifier la séance puisque toi seule connais le code secret que tu partages avec ton contact, et ce dernier devrait être alerté à ce stade de la communication. C'est la raison pour laquelle l'authentification est tellement importante. De plus, si tu as suivi pas à pas les instructions et as adéquatement configuré l'onglet "Configuration" d'OTR avec les préférences recommandées, même si une personne te vole ton mot de passe, elle n'aura pas accès à tes conversations passées, puisque tu as choisi de ne pas les archiver.*

5.1 Questions récapitulatives

1. Quelles sont les configurations informatiques requises pour la création d'un compte dans Pidgin?
2. Est-il possible d'enregistrer et utiliser plusieurs compte de messagerie instantanée simultanément avec Pidgin?
3. Quels sont les configurations requises pour l'ouverture d'une séance de clavardage sécurisée et confidentielle dans Pidgin?
4. Combien de fois est-il nécessaire d'authentifier une séance de clavardage avec un contact donné?
5. Qu'est-ce qu'une empreinte, dans Pigin?
6. Qu'advient-il de vos préférences OTR (y compris les empreintes reçues) lorsque vous installez Pidgin et OTR sur un autre ordinateur?

VaultletSuite - client de courriel sécurisé

VaultletSuite 2 Go (**VS2Go**) est un programme de courrier électronique sécurisé qui vous donne la possibilité de stocker vos messages de courriel et autres fichiers sur votre ordinateur, sur une clé USB ou sur le serveur de VaultletSoft.

Site Internet

www.vaultletsoft.com [137]

Configuration requise :

- Windows 2000/XP/Vista

Pour installer VaultletSuite

- *Lisez la courte introduction des Guides pratiques [13]*
- ***Cliquez sur l'icône ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez*

- Une connexion Internet

Version utilisée pour rédiger ce guide :

- 2.7.9 (peut différer)

Licence :

- Gratuiciel (*Freeware*)

d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

VaultletSuite:

[138]

Lecture préalable :

- Livret pratique Security in-a-box, chapitre 7. Préserver la confidentialité de vos communications sur Internet [127].

Niveau : 1 : Débutant, 2 : Moyen, **3 : Intermédiaire**, 4 : Expérimenté, 5 : Avancé

Temps d'apprentissage : 60 minutes

Ce que vous apportera l'utilisation de cet outil :

- Un programme de courrier électronique sécurisé, qui chiffre automatiquement vos messages et fichiers.
- La capacité de déterminer comment vos messages de courriel sont lus par le(s) destinataire(s). Par exemple, vous pouvez faire en sorte qu'il soit impossible de transférer les courriels que vous envoyez à d'autres destinataires, ou encore configurer les messages pour qu'ils soient automatiquement supprimés après la première lecture.
- La possibilité d'envoyer des messages chiffrés à n'importe quelle adresse de courriel, sans qu'il soit nécessaire pour vos destinataires d'utiliser VaultletSoft ou un autre outil particulier pour les lire.
- La capacité de transporter avec vous vos messages et fichiers en les stockant de façon sécurisée sur une clé USB.

1.1 À propos de cet outil

VaultletSuite 2 Go (**VS2Go**) est un programme de courrier électronique sécurisé qui vous donne la possibilité de stocker vos messages de courriel et autres fichiers sur votre ordinateur, sur une clé USB ou sur un serveur de VaultletSoft. Pour fonctionner normalement, VS2Go doit installer la plateforme **Java** sur votre ordinateur. Ce logiciel a une apparence un peu différente des autres programmes de messagerie avec lesquels vous êtes déjà familier, et votre compte de courriel n'est pas accessible via un navigateur Internet.

VS2Go est une suite logicielle composée de trois produits complémentaires, accessibles par une console unique :

- **VaultletMail** – le client de messagerie
- **PasswordValet** – l'outil de gestion des mots passe
- **VaultletFiler** – l'outil de chiffrement des fichiers

VS2Go utilise la méthode de chiffrement asymétrique (par clé publique) pour assurer la sécurité de vos communications et de vos données. Vous pouvez en apprendre davantage sur cette méthode de chiffrement en lisant le chapitre 7. Préserver la confidentialité de vos communications sur Internet [127] du livret pratique. Toutes les tâches de chiffrement sont effectuées automatiquement pour vous par le logiciel VS2Go. Cela accroît le niveau de sécurité de vos communications en réduisant le facteur d'erreur humaine, tout en facilitant l'utilisation du programme.

VS2Go offre un peu d'espace sur ses serveurs pour vos messages de courriel. Les nouveaux messages y seront stockés et pourront être relevés à partir de n'importe quel ordinateur où le logiciel VS2Go est installé. Néanmoins, vous devriez créer une archive locale sur votre ordinateur ou sur une clé USB et y transférer régulièrement vos messages. L'archive locale n'est limitée que par son volume.

Comment créer un compte VS2Go

Commentaire sur l'installation : Après avoir installé VS2Go et lancé le programme une première fois, il est possible que vous receviez des requêtes de mise à jour vous invitant à installer la plus récente version. Veuillez consulter la section **2.3 Sur l'actualisation de VS2Go** pour connaître la procédure à suivre lorsque cela se produit.

Votre compte VS2Go comprend une adresse de courriel et des renseignements de connexions pour le système. Vous pouvez enregistrer plusieurs comptes sur le même ordinateur. Chaque compte dispose d'un espace séparé et est protégé contre les accès de non propriétaires.

Première étape. **Cliquez** sur : ou **sélectionnez : Démarrer > Programmes > VaultletSuite2Go > VaultletSuite2Go** pour activer la console principale de *VaultletSuite 2 Go* et la fenêtre *Bienvenue à VaultletSuite 2 Go* :

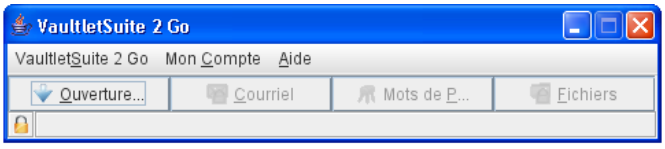


Figure 1 : La console principale deVaultletSuite 2 Go

La console de *VS2Go* vous permet de naviguer entre le programme de courriel, l'outil de stockage de fichiers et l'outil de gestion de mots de passe de VaultletSuite. Vous devez toutefois créer un compte avant de pouvoir commencer à utiliser ces outils.

Figure 2 : La fenêtre Bienvenue à VaultletSuite 2 Go

Deuxième étape. **Cliquez** sur : pour afficher la fenêtre suivante.

La fenêtre *Choisissez le mode de création de compte que vous souhaitez utiliser* est abordée plus en détails à la prochaine section.

2.1 Comment choisir le bon compte VS2Go

VaultletSuite vous offre la possibilité de stocker votre compte et vos renseignements de connexion sur votre ordinateur ou sur une clé USB. Cette option sert à accommoder aussi bien les personnes qui utilisent toujours le même ordinateur que celles qui utilisent plusieurs ordinateurs différents, et ce, sans pour autant compromettre leur sécurité.

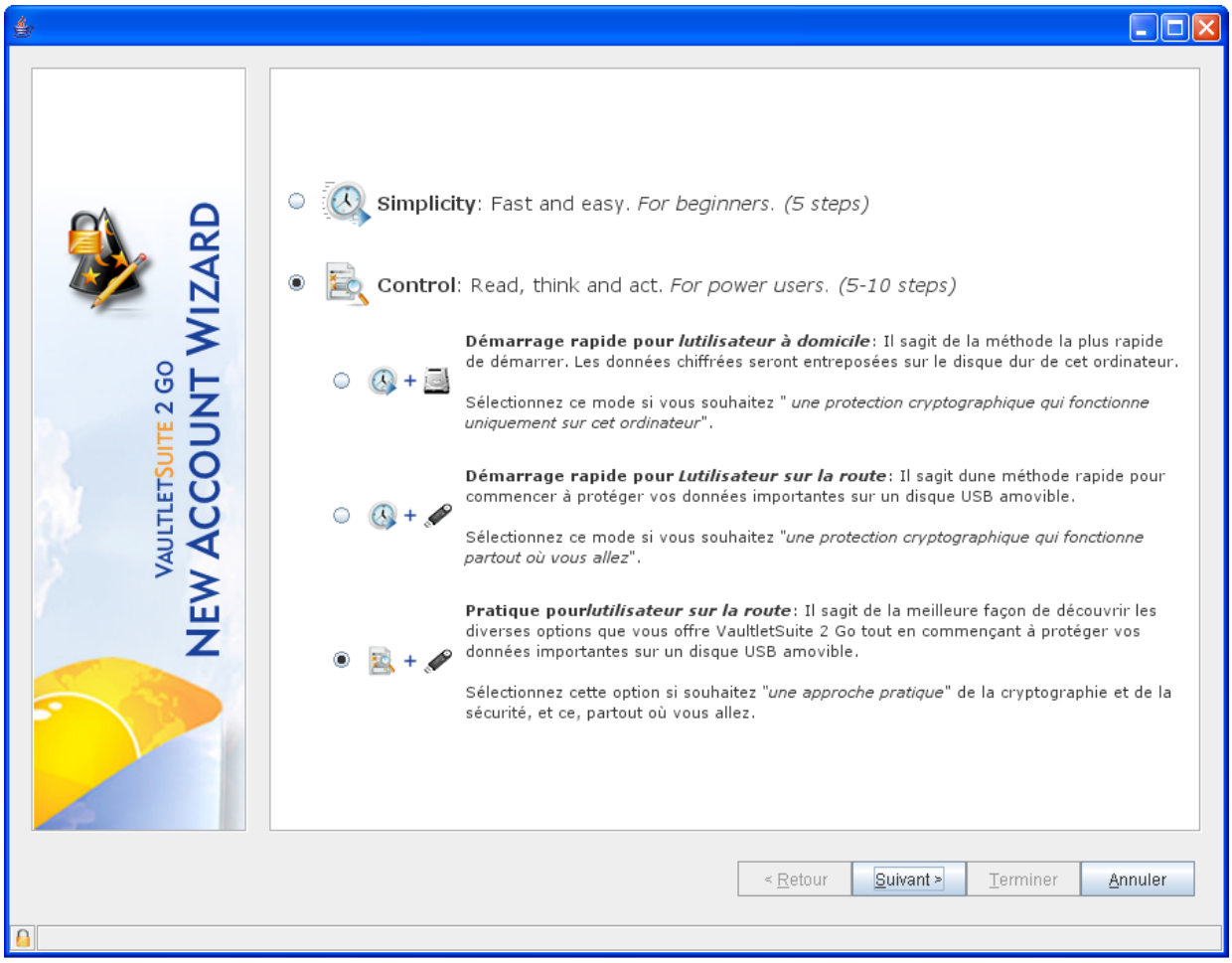

VAULTLETSUITE 2 GO
NEW ACCOUNT WIZARD
Simplicity: Fast and easy. For beginners. (5 steps)
Control: Read, think and act. For power users. (5-10 steps)
Démarrage rapide pour lutilisateur à domicile: Il sagit de la méthode la plus rapide de démarrer. Les données chiffrées seront entreposées sur le disque dur de cet ordinateur.
Sélectionnez ce mode si vous souhaitez " une protection cryptographique qui fonctionne uniquement sur cet ordinateur".
Démarrage rapide pour Lutilisateur sur la route: Il sagit dune méthode rapide pour commencer à protéger vos données importantes sur un disque USB amovible.
Sélectionnez ce mode si vous souhaitez "une protection cryptographique qui fonctionne partout où vous allez".
Pratique pourlutilisateur sur la route: Il sagit de la meilleure façon de découvrir les diverses options que vous offre VaultletSuite 2 Go tout en commençant à protéger vos données importantes sur un disque USB amovible.
Sélectionnez cette option si souhaitez "une approche pratique" de la cryptographie et de la sécurité, et ce, partout où vous allez.
< Retour
Suivant >
Terminer
Annuler

Figure 3 : La fenêtre Choisissez le mode de création de compte que vous souhaitez utiliser

Important : Veuillez lire les descriptions des différentes options avant de choisir celles qui correspond le mieux à vos besoins.

- L'option *Simplicité. Rapide et facile. Pour débutants* est appropriée pour les utilisateurs qui sont satisfaits avec les options par défaut lors de l'enregistrement du compte. Vous devrez fournir un minimum de renseignements. Le compte sera stocké dans le répertoire 'home' de votre ordinateur (par exemple - C:Documents and SettingsUservaultletsoft) et la clé privée sera stockée sur le serveur de VaultletSoft.

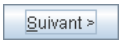
- L'option *Contrôle: Démarrage rapide pour l'utilisateur à domicile* crée un compte par la même procédure de configuration qu'avec l'option *Simplicité*, mais donne davantage de détails sur les choix liés à l'installation et à l'accès au

système.

- L'option *Contrôle: Démarrage rapide pour l'utilisateur sur la route (6 étapes)* est conçu pour faciliter un processus d'enregistrement rapide, en tenant pour acquis que vos courriels et fichiers seront sauvegardés sur une clé USB. Choisissez cette option si vous souhaitez transporter votre compte VS2Go avec vous et y accéder à partir de plusieurs ordinateurs différents.
- L'option *Contrôle: Pratique, pour l'utilisateur sur la route (10 étapes)* est appropriée pour les utilisateurs qui veulent étudier attentivement toutes les options avant de choisir la configuration qui leur convient le mieux. Vous pouvez aussi choisir l'emplacement où sera stockée votre clé privée.

Commentaire : Dans le présent guide, nous ferons la démonstration d'un enregistrement avec l'option *Pratique pour l'utilisateur sur la route*, avec des réglages qui seront appropriés pour la plupart des utilisateurs. Pour ceux qui préfèrent choisir un autre mode d'enregistrement de compte, veuillez tout de même étudier attentivement la prochaine section pour avoir une meilleure idée des étapes importantes.

Première étape. **Sélectionnez** le mode de création de compte qui convient le mieux à vos besoins.

Deuxième étape. **Cliquez** sur : 

2.2 Procédure d'enregistrement pas à pas

Cette section fait la démonstration d'un enregistrement d'un compte VS2Go avec l'option *Pratique pour l'utilisateur sur la route*.

Pour commencer, il vous faut générer votre paire de clés. Ce sera la principale mesure de sécurité de votre compte.

Première étape. **Rattrapez** le carré coloré avec votre souris!

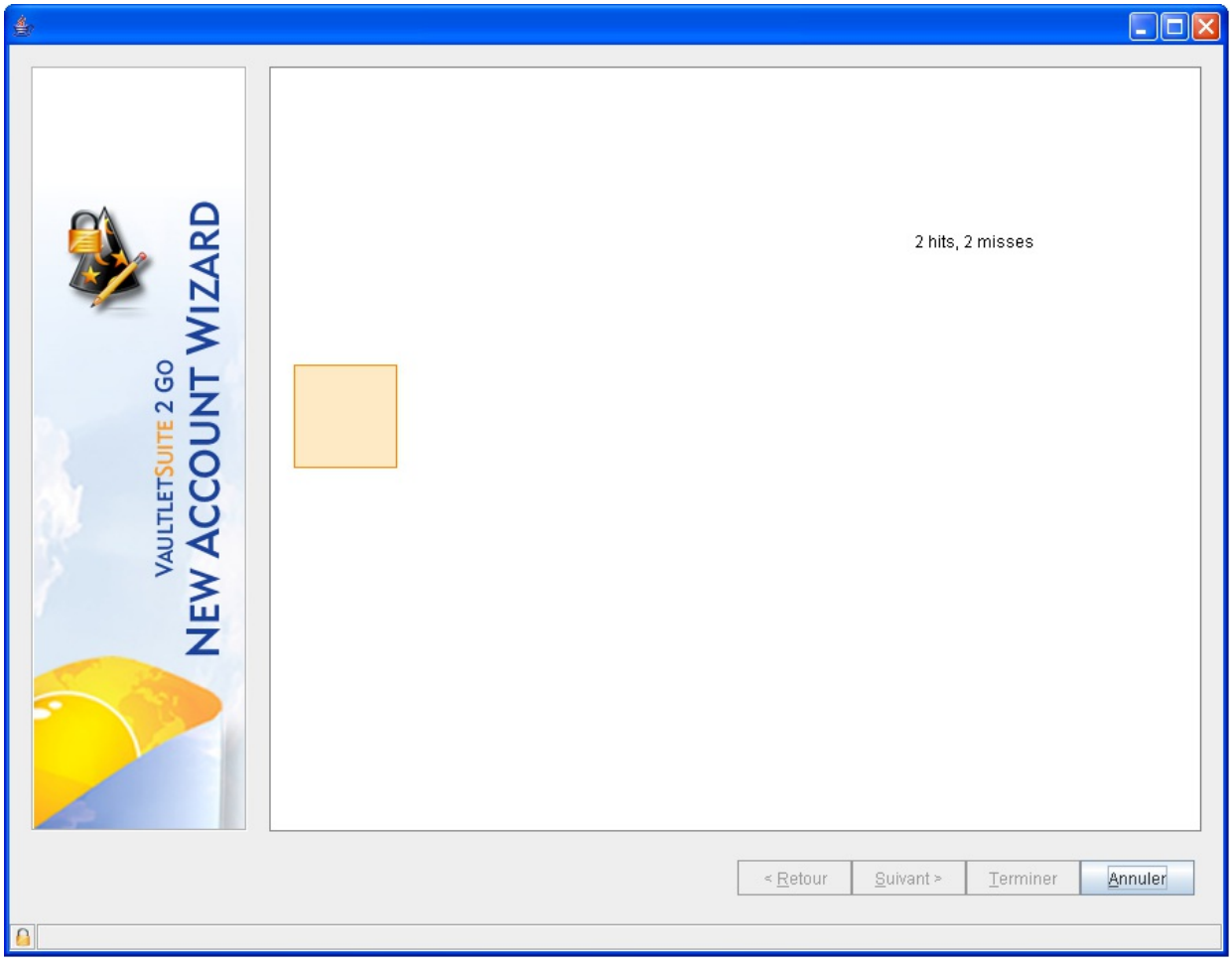


Figure 4 : La fenêtre du générateur de paires de clé

Deuxième étape. **Choisissez** un emplacement où stocker votre clé privée.

Commentaire : N'oubliez pas que votre clé privée est le seul moyen dont vous disposez pour déchiffrer les messages et les fichiers dans votre compte. Si vous choisissez de la sauvegarder localement (l'option Contrôle, voir ci-dessus) – sur votre ordinateur ou sur une clé USB – assurez-vous de ne pas perdre ou endommager ce fichier. Il ne vous sera pas possible de remplacer votre clé privée si vous perdez ou endommagez l'originale. Cette option est appropriée pour les utilisateurs expérimentés qui sont confiants d'être en mesure de gérer leur clé privée de façon sûre. Si vous décidez de sauvegarder votre clé privée sur les serveurs de VaultletSoft (l'option Simplicité, voir ci-dessus), vous n'aurez plus à vous soucier de la perdre ou d'en conserver une copie chaque fois que vous souhaitez accéder à votre compte. La responsabilité de conserver votre clé privée reposera sur la compagnie VaultletSoft. Par contre, dans ce dernier scénario, vous devrez créer une phrase secrète exceptionnellement longue afin de protéger votre clé. Pour plus de renseignements au sujet des clés publiques et privées, veuillez consulter le chapitre 7. Préserver la confidentialité de vos communications sur Internet [127] du livret pratique.

Troisième étape. **Sélectionnez** l'option *Simplicité*

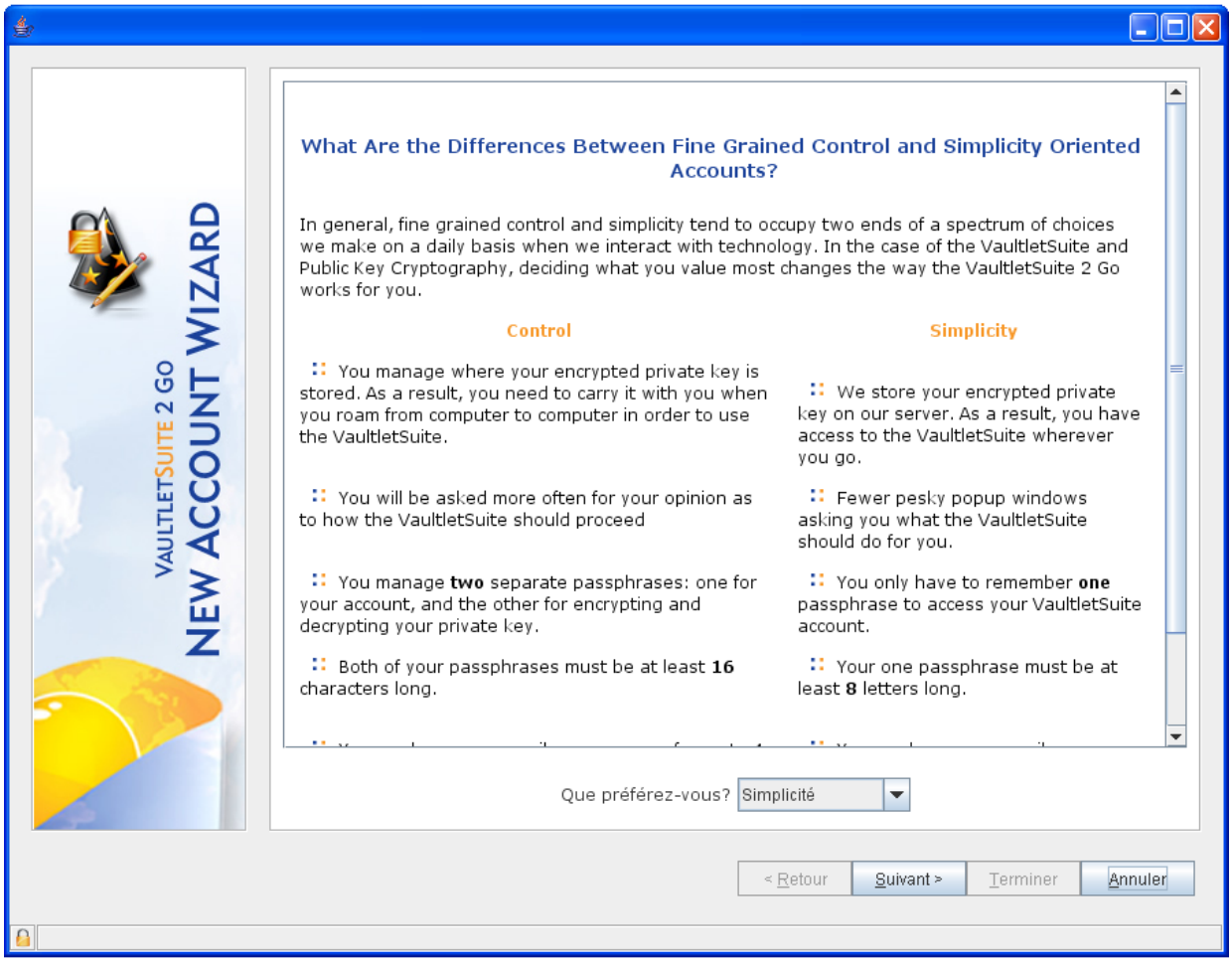
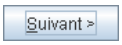

VAULTLETSUITE 2 GO
NEW ACCOUNT WIZARD
What Are the Differences Between Fine Grained Control and Simplicity Oriented Accounts?
In general, fine grained control and simplicity tend to occupy two ends of a spectrum of choices we make on a daily basis when we interact with technology. In the case of the VaultletSuite and Public Key Cryptography, deciding what you value most changes the way the VaultletSuite 2 Go works for you.
Control
Simplicity
You manage where your encrypted private key is stored. As a result, you need to carry it with you when you roam from computer to computer in order to use the VaultletSuite.
We store your encrypted private key on our server. As a result, you have access to the VaultletSuite wherever you go.
You will be asked more often for your opinion as to how the VaultletSuite should proceed
Fewer pesky popup windows asking you what the VaultletSuite should do for you.
You manage two separate passphrases: one for your account, and the other for encrypting and decrypting your private key.
You only have to remember one passphrase to access your VaultletSuite account.
Both of your passphrases must be at least 16 characters long.
Your one passphrase must be at least 8 letters long.
Que préférez-vous? Simplicité
< Retour
Suivant >
Terminer
Annuler

Figure 5: Choisissez un mode d'enregistrement

Quatrième étape. **Cliquez** sur :  pour continuer.

Il est possible que vous voyiez apparaître une fenêtre vous présentant la licence gratuite pour les organismes à but non lucratif. La prochaine fenêtre est celle de l'enregistrement du compte. Choisissez un nom pour le compte et une phrase secrète (mot de passe), et saisissez les autres renseignements demandés.

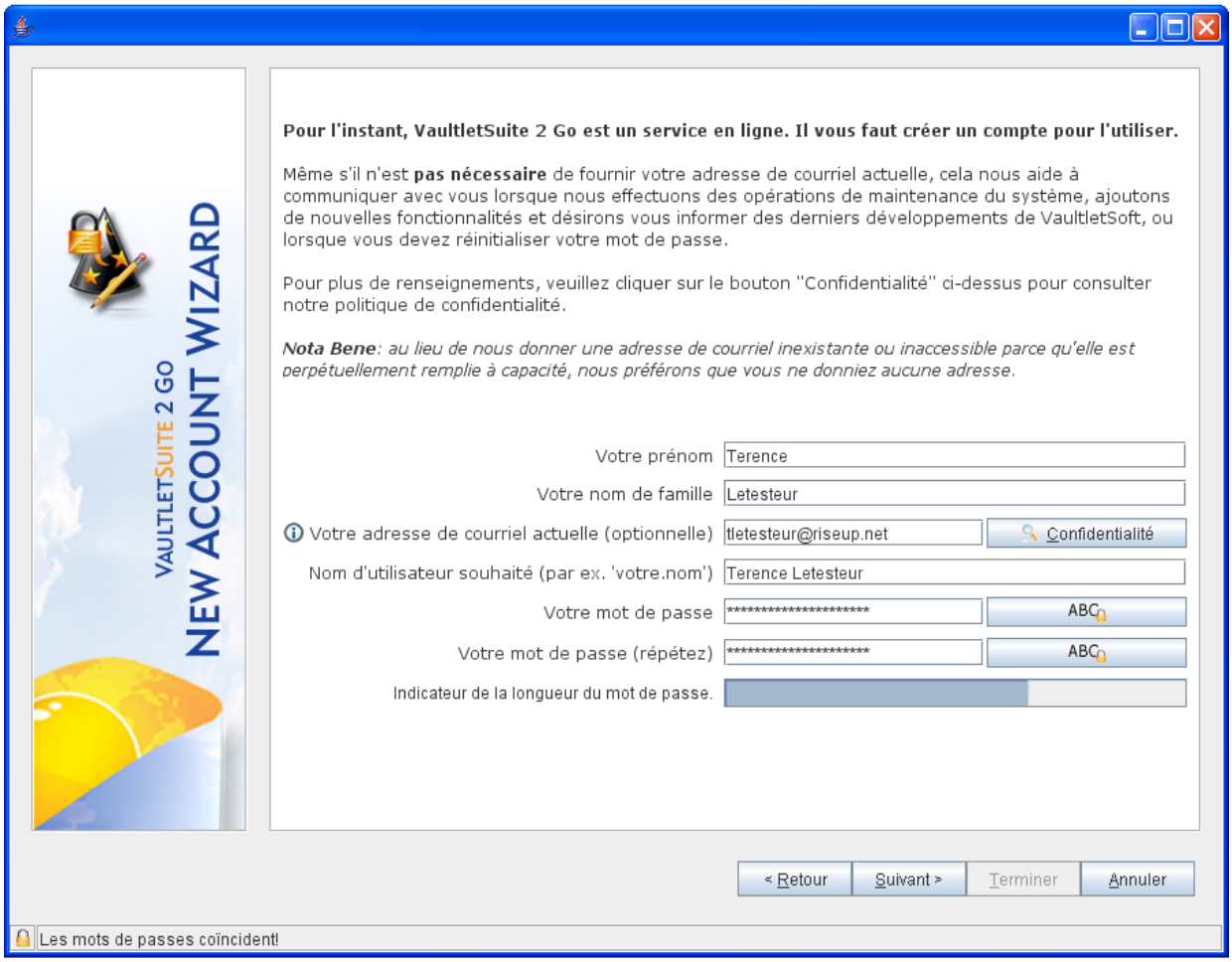

VAULTLETSUITE 2 GO
NEW ACCOUNT WIZARD
Pour l'instant, VaultletSuite 2 Go est un service en ligne. Il vous faut créer un compte pour l'utiliser.
Même s'il n'est pas nécessaire de fournir votre adresse de courriel actuelle, cela nous aide à communiquer avec vous lorsque nous effectuons des opérations de maintenance du système, ajoutons de nouvelles fonctionnalités et désirons vous informer des derniers développements de VaultletSoft, ou lorsque vous devez réinitialiser votre mot de passe.
Pour plus de renseignements, veuillez cliquer sur le bouton "Confidentialité" ci-dessus pour consulter notre politique de confidentialité.
Nota Bene: au lieu de nous donner une adresse de courriel inexistante ou inaccessible parce qu'elle est perpétuellement remplie à capacité, nous préférons que vous ne donniez aucune adresse.
Votre prénom
Terence
Votre nom de famille
Letesteur
Votre adresse de courriel actuelle (optionnelle)
tletesteur@riseup.net
Confidentialité
Nom d'utilisateur souhaité (par ex. 'votre.nom')
Terence Letesteur
Votre mot de passe
Votre mot de passe (répétez)
ABC
Indicateur de la longueur du mot de passe.
< Retour
Suivant >
Terminer
Annuler
Les mots de passes coïncident!

Figure 6 : Le formulaire de création de compte

Cinquième étape. **Saisissez** les renseignements requis dans les zones appropriées.

Votre adresse de courriel actuelle sera utilisée pour réinitialiser votre phrase secrète ou pour vous communiquer des annonces importantes concernant votre compte.

Commentaire : Si vous souhaitez accroître le niveau d'anonymat de votre compte VS2Go, vous pouvez enregistrer un nom fictif et omettre l'adresse de courriel alternative. N'oubliez pas, cependant, que si vous n'indiquez pas d'adresse de courriel de rechange, vous ne serez pas en mesure de réinitialiser votre phrase secrète (mot de passe) si vous l'oubliez ou la perdez.

Votre **Nom d'utilisateur souhaité** ne doit pas contenir d'espaces et doit être complètement original. Ce nom sera utilisé dans votre adresse de courriel VS2Go. *Par exemple* : terrence.letesteur@vaultletsoft.com [139]

Commentaire : VS2Go vous offre une méthode sûre pour saisir votre mot de passe : le clavier virtuel. Cette option permet de protéger votre phrase secrète contre les enregistreurs de frappe qui pourraient être installés sur l'ordinateur que vous utilisez.

Sixième étape. **Cliquez** sur : pour activer le *Clavier virtuel* :

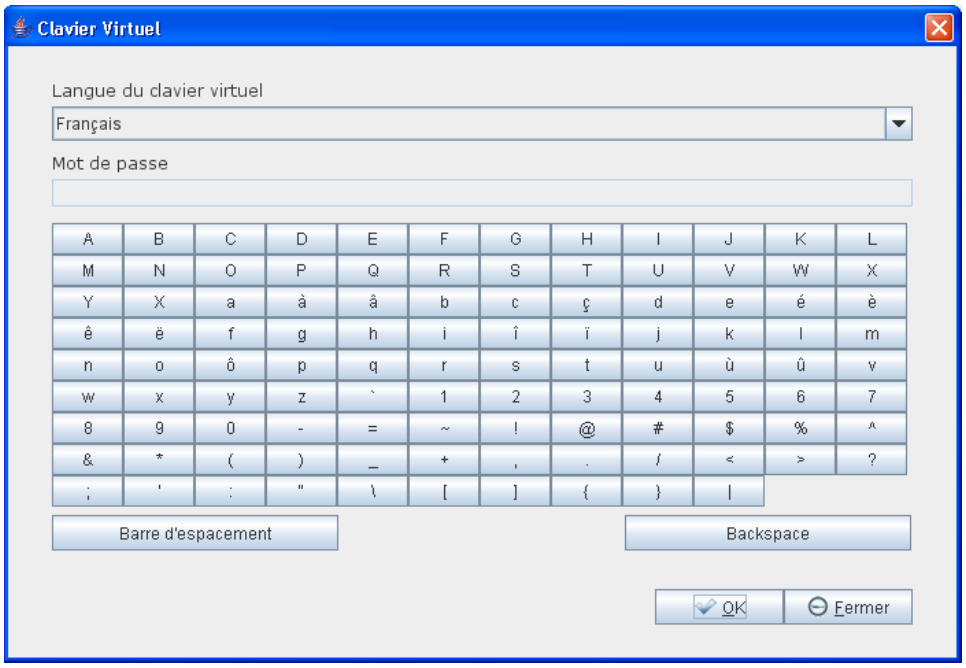
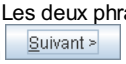


Figure 7 : Le clavier virtuel

Septième étape. **Cliquez** sur les touches correspondant à votre phrase secrète sur le *clavier virtuel*.

Huitième étape. **Cliquez** sur : lorsque vous avez terminé.

Neuvième étape. **Saisissez** une seconde fois votre phrase secrète à l'aide du clavier virtuel. Les deux phrases doivent correspondre et doivent comprendre au moins 8 caractères. Lorsque tout concorde, le bouton  est activé et vous pouvez poursuivre le processus d'enregistrement.

La prochaine fenêtre présente le *contrat d'utilisation*.

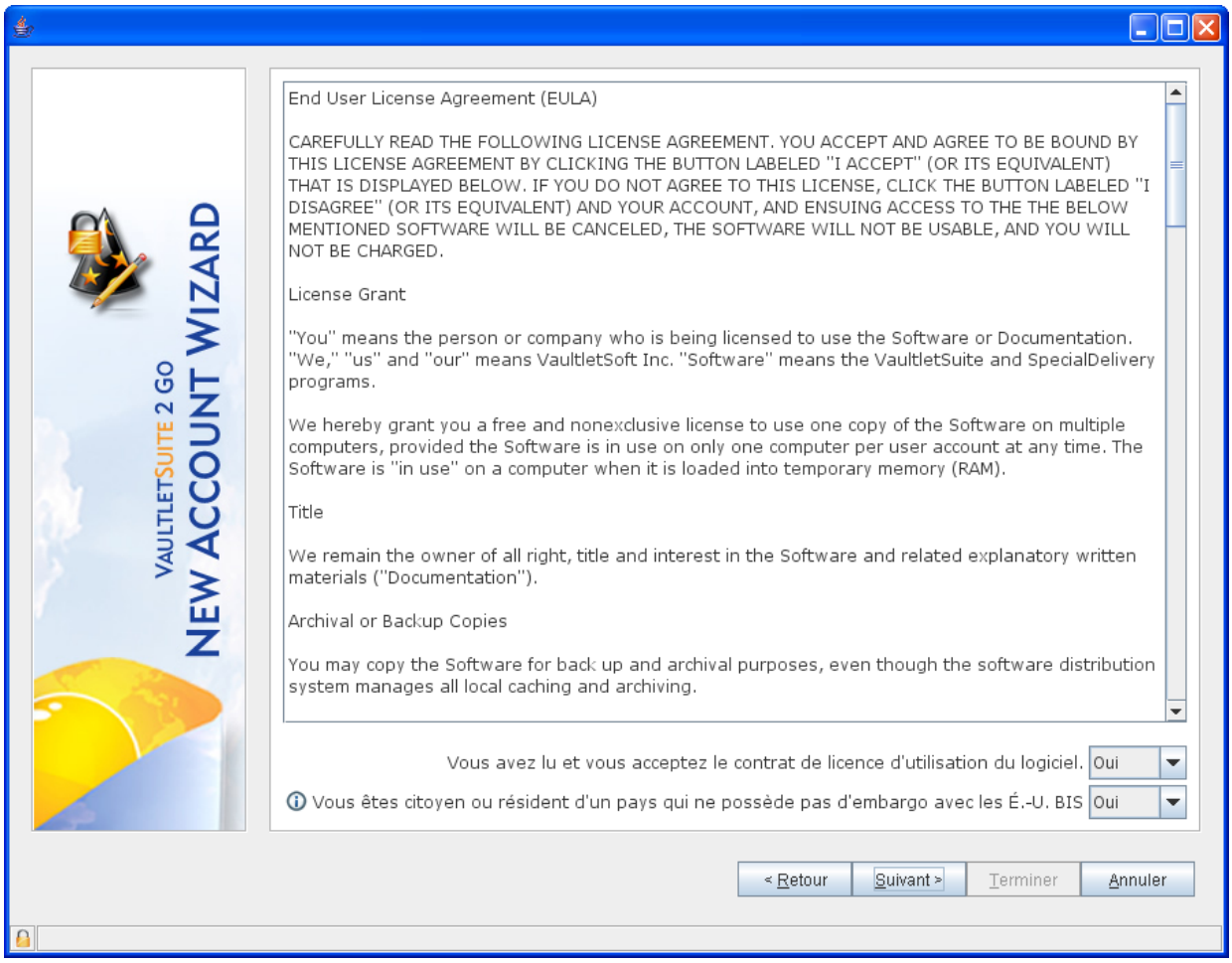

VAULTLETSUITE 2 GO
NEW ACCOUNT WIZARD
End User License Agreement (EULA)
CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT. YOU ACCEPT AND AGREE TO BE BOUND BY THIS LICENSE AGREEMENT BY CLICKING THE BUTTON LABELED "I ACCEPT" (OR ITS EQUIVALENT) THAT IS DISPLAYED BELOW. IF YOU DO NOT AGREE TO THIS LICENSE, CLICK THE BUTTON LABELED "I DISAGREE" (OR ITS EQUIVALENT) AND YOUR ACCOUNT, AND ENSUING ACCESS TO THE THE BELOW MENTIONED SOFTWARE WILL BE CANCELED, THE SOFTWARE WILL NOT BE USABLE, AND YOU WILL NOT BE CHARGED.
License Grant
"You" means the person or company who is being licensed to use the Software or Documentation. "We," "us" and "our" means VaultletSoft Inc. "Software" means the VaultletSuite and SpecialDelivery programs.
We hereby grant you a free and nonexclusive license to use one copy of the Software on multiple computers, provided the Software is in use on only one computer per user account at any time. The Software is "in use" on a computer when it is loaded into temporary memory (RAM).
Title
We remain the owner of all right, title and interest in the Software and related explanatory written materials ("Documentation").
Archival or Backup Copies
You may copy the Software for back up and archival purposes, even though the software distribution system manages all local caching and archiving.
Vous avez lu et vous acceptez le contrat de licence d'utilisation du logiciel.
Oui
Vous êtes citoyen ou résident d'un pays qui ne possède pas d'embargo avec les É.-U. BIS
Oui
< Retour
Suivant >
Terminer
Annuler

Figure 8 : La fenêtre du contrat d'utilisation

Dixième étape. **Sélectionnez** *Oui* dans les deux menus pour continuer.

La prochaine fenêtre présente les renseignements concernant les bénéficiaires et référents de VS2Go.

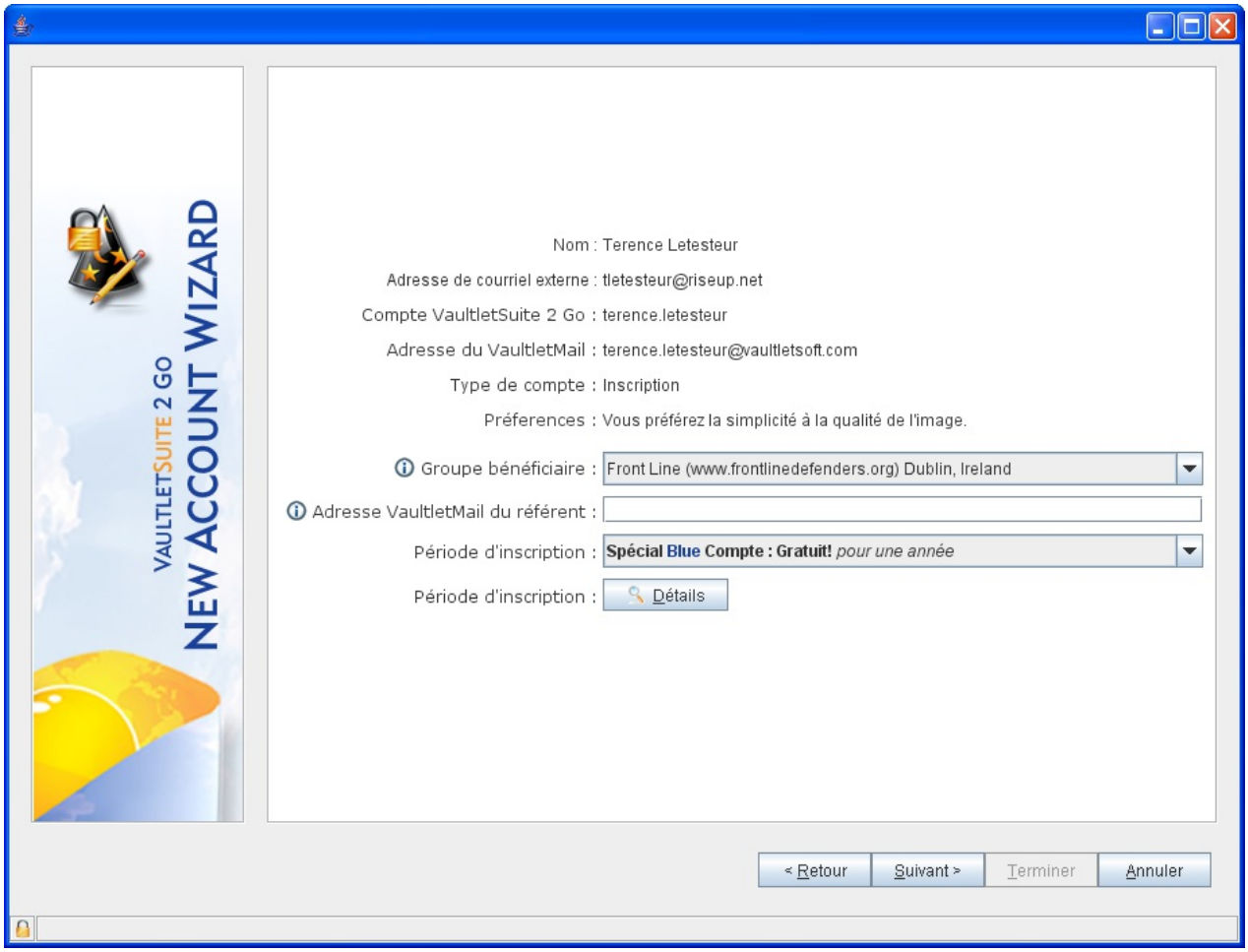

VAULTLETSUITE 2 GO
NEW ACCOUNT WIZARD
Nom : Terence Letesteur
Adresse de courriel externe : tletesteur@riseup.net
Compte VaultletSuite 2 Go : terence.letesteur
Adresse du VaultletMail : terence.letesteur@vaultletsoft.com
Type de compte : Inscription
Préferences : Vous préférez la simplicité à la qualité de l'image.
Groupe bénéficiaire : Front Line (www.frontlinedefenders.org) Dublin, Ireland
Adresse VaultletMail du référent :
Période d'inscription : Spécial Blue Compte : Gratuit! pour une année
Période d'inscription : Détails
< Retour
Suivant >
Terminer
Annuler

Figure 9 : La fenêtre des bénéficiaires et référents

Onzième étape. **Sélectionnez** le groupe bénéficiaire auquel vous souhaitez que VaultletSoft? achemine ses dons et offre son soutien.

Douzième étape. **Sélectionnez** le compte *Special Blue* dans le menu *Période d'inscription*.

Commentaire : Ce type de compte vous donnera accès à la plupart des fonctions de VaultletSuite pour une période d'un an. Après onze mois, vous recevrez un courriel vous rappelant que votre période d'inscription d'un an tire à sa fin. Veuillez consulter la **Section 5. FAQ et questions récapitulatives** [140] pour plus de renseignements sur les moyens de prolonger votre période d'inscription.

Treizième étape. **Cliquez** sur : Suivant > pour activer la fenêtre suivante :

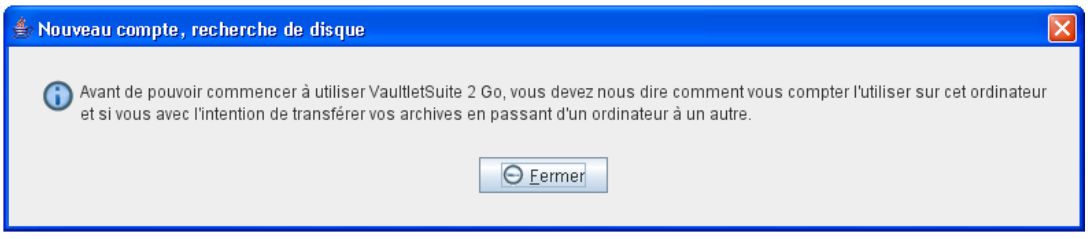

Nouveau compte, recherche de disque
Avant de pouvoir commencer à utiliser VaultletSuite 2 Go, vous devez nous dire comment vous compter l'utiliser sur cet ordinateur et si vous avec l'intention de transférer vos archives en passant d'un ordinateur à un autre.
Fermer

Figure 10 : La fenêtre de recherche de disque pour un nouveau compte

Quatorzième tape. **Cliquez** sur le bouton *Fermer* pour activer la fenêtre de *recherche de disque*.

Vous devez maintenant choisir l'emplacement où les fichiers VS2Go seront stockés.

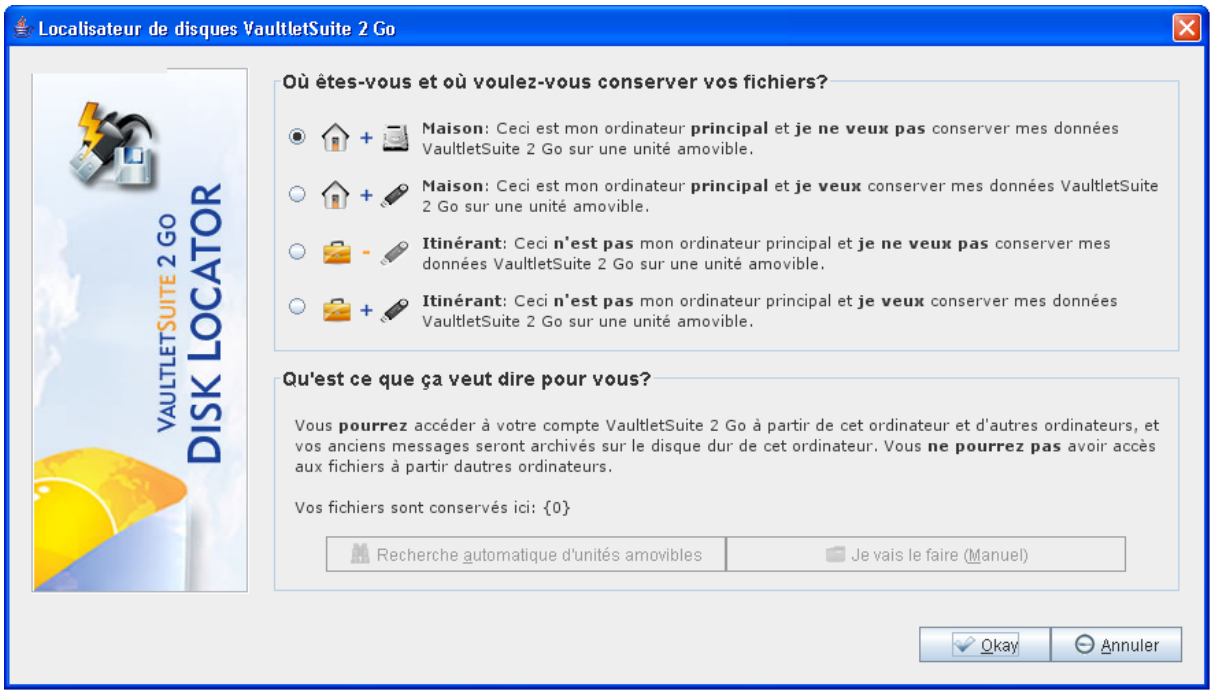

Localisateur de disques VaultletSuite 2 Go
VAULTLETSUITE 2 GO
DISK LOCATOR
Où êtes-vous et où voulez-vous conserver vos fichiers?
Maison: Ceci est mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible.
Maison: Ceci est mon ordinateur principal et je veux conserver mes données VaultletSuite 2 Go sur une unité amovible.
Itinérant: Ceci n'est pas mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible.
Itinérant: Ceci n'est pas mon ordinateur principal et je veux conserver mes données VaultletSuite 2 Go sur une unité amovible.
Qu'est ce que ça veut dire pour vous?
Vous pourrez accéder à votre compte VaultletSuite 2 Go à partir de cet ordinateur et d'autres ordinateurs, et vos anciens messages seront archivés sur le disque dur de cet ordinateur. Vous ne pourrez pas avoir accès aux fichiers à partir dautres ordinateurs.
Vos fichiers sont conservés ici: {0}
Recherche automatique d'unités amovibles
Je vais le faire (Manuel)
Okay
Annuler

Figure 11 : La fenêtre Où êtes-vous et où voulez-vous conserver vos fichiers de VaultletSuite 2 Go

Choisissez l'une des trois options de stockage de fichiers :

Vous pouvez conserver les fichiers de votre compte VS2G0 sur votre ordinateur, sur un serveur de Vaultlet ou sur une clé USB. Chacune des options est détaillée dans cette fenêtre, et vous pouvez lire de plus amples explications en **cochant** l'une ou l'autre. N'oubliez pas que si vous choisissez de conserver vos fichiers sur une clé USB, vous ne serez pas en mesure d'accéder à votre compte ou à vos archives à moins que vous ne transportiez la clé USB avec vous.

Option 1 *– Je désire sauvegarder tous mes fichier et y accéder sur mon ordinateur seulement* .

Comme le nom le suggère, vous ne pourrez accéder à votre compte qu'à partir de votre ordinateur.

Première étape. **Cochez** l'option *Maison : ceci est mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible*.

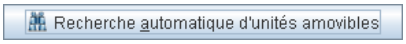
Deuxième étape. **Cliquez** sur : pour continuer.

Option 2 *– Je désire conserver les données de mon compte et y accéder sur une clé USB*

Si vous souhaitez accéder à VS2Go à partir de plusieurs ordinateurs différents (le logiciel VS2Go devra être installé sur chaque ordinateur utilisé), choisissez cette option et transportez les données du compte avec vous sur une clé USB.

Première étape. **Cochez** l'option 'Maison: ceci est mon ordinateur principal et je veux conserver mes données VaultletSuite 2 Go sur ma clé USB'.

Vous devrez alors indiquer à VS2Go où se trouve votre clé USB.

Deuxième étape. **Cliquez** sur : 

VS2Go effectuera une recherche sur votre ordinateur pour détecter des unités de stockage amovible. Si plus d'une unité sont trouvées, vous devrez en sélectionner une seule.

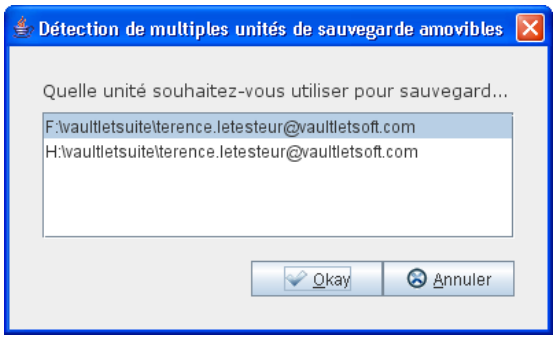


Figure 12 : La fenêtre Détection de multiples unités de stockage amovibles

Cette fenêtre devrait alors apparaître :

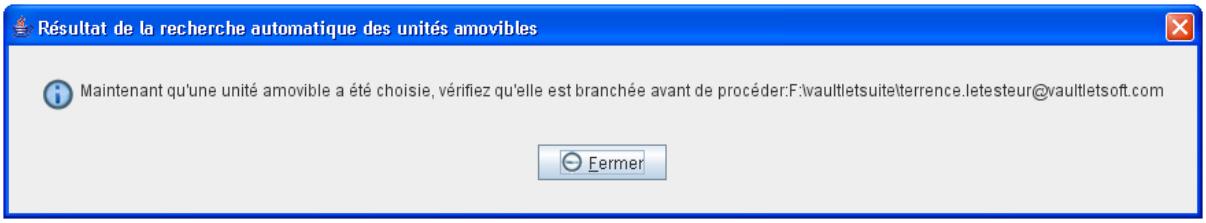

Résultat de la recherche automatique des unités amovibles
Maintenant qu'une unité amovible a été choisie, vérifiez qu'elle est branchée avant de procéder:F:\vaultletsuite\terrence.letesteur@vaultletsoft.com
Fermer

Figure 13 : La fenêtre Résultat de la recherche automatique des unités amovibles

La fenêtre de *Détection d'unités amovibles* affichera maintenant l'emplacement de votre clé USB, ainsi que le répertoire suggéré pour le stockage de vos données.

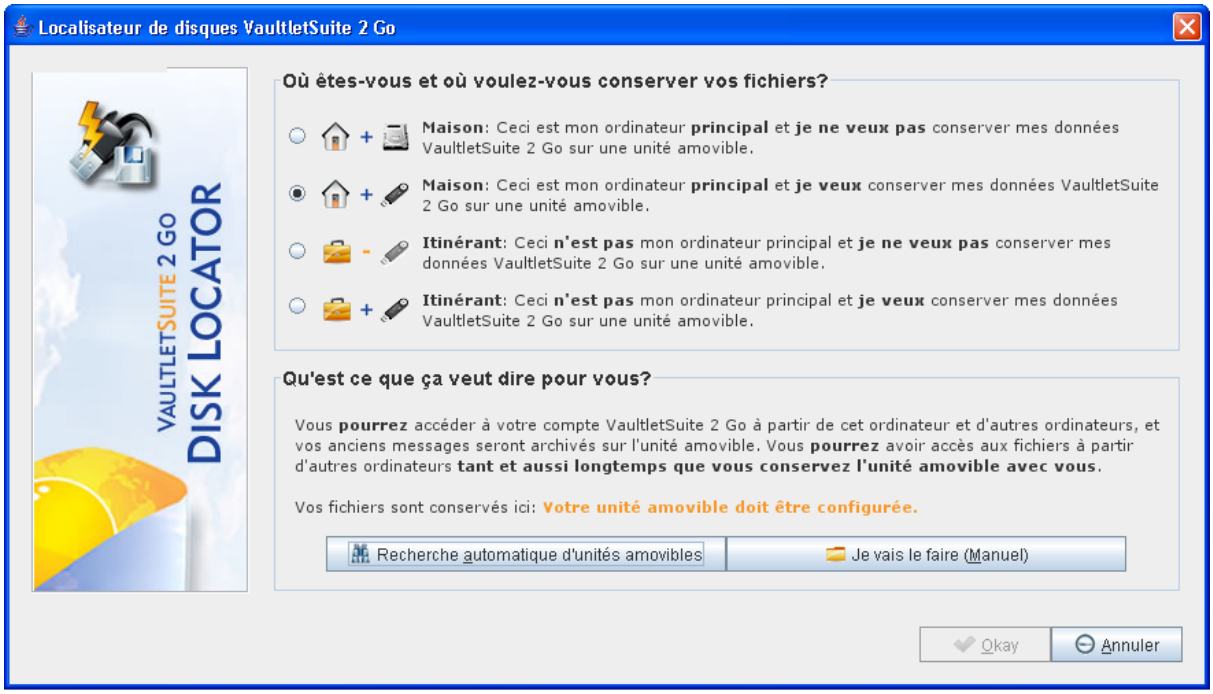

Localisateur de disques VaultletSuite 2 Go
VAULTLETSUITE 2 GO
DISK LOCATOR
Où êtes-vous et où voulez-vous conserver vos fichiers?
Maison: Ceci est mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible.
Maison: Ceci est mon ordinateur principal et je veux conserver mes données VaultletSuite 2 Go sur une unité amovible.
Itinérant: Ceci n'est pas mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible.
Itinérant: Ceci n'est pas mon ordinateur principal et je veux conserver mes données VaultletSuite 2 Go sur une unité amovible.
Qu'est ce que ça veut dire pour vous?
Vous pourrez accéder à votre compte VaultletSuite 2 Go à partir de cet ordinateur et d'autres ordinateurs, et vos anciens messages seront archivés sur l'unité amovible. Vous pourrez avoir accès aux fichiers à partir d'autres ordinateurs tant et aussi longtemps que vous conserverez l'unité amovible avec vous.
Vos fichiers sont conservés ici: Votre unité amovible doit être configurée.
Recherche automatique d'unités amovibles
Je vais le faire (Manuel)
Okay
Annuler

Figure 14 : La fenêtre Où êtes-vous et où voulez-vous conserver vos fichiers de VaultletSuite 2 Go

Si vous souhaitez changer le répertoire par défaut ou choisir une autre unité de stockage :

Troisième étape. **Cliquez** sur :

et sélectionnez l'emplacement désiré.

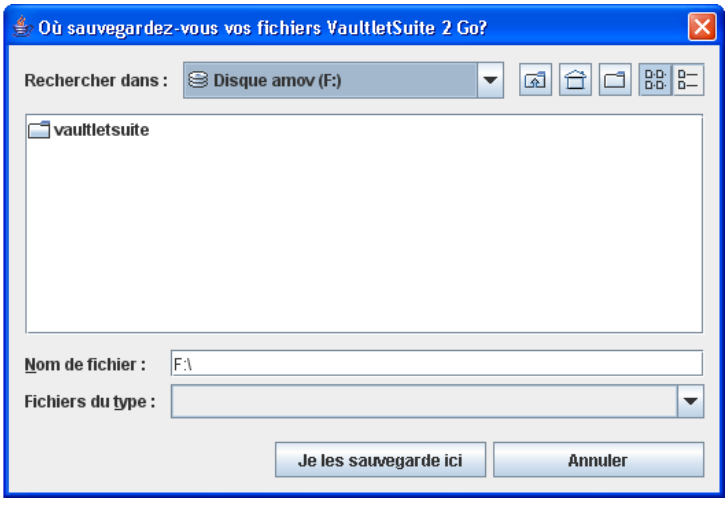
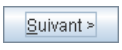


Figure 15 : La fenêtre Où sauvegardez-vous vos fichiers VaultletSuite 2 Go

Quatrième étape. **Cliquez** sur : 

pour continuer.

Commentaire : Si vous choisissez de transporter les données du compte sur une clé USB, vous devrez la connecter à l'ordinateur avant de lancer le programme VS2Go. Vous devrez peut-être préciser son emplacement si vous vous êtes déjà connecté à partir d'autres ordinateurs.

Option 3 *– Je veux simplement recevoir et envoyer quelques nouveaux messages. Je n'ai pas besoin d'accéder à mes archives.*

Première étape. **Cochez** l'option *Itinérant: Ceci n'est pas mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible*.

Deuxième étape. **Cliquez** sur : Suivant >

Finaliser l'enregistrement de votre compte VS2Go

Finalement, une fenêtre vous présente une vue d'ensemble de votre nouveau compte Vaultletsoft. Assurez-vous que tous les renseignements sont corrects.

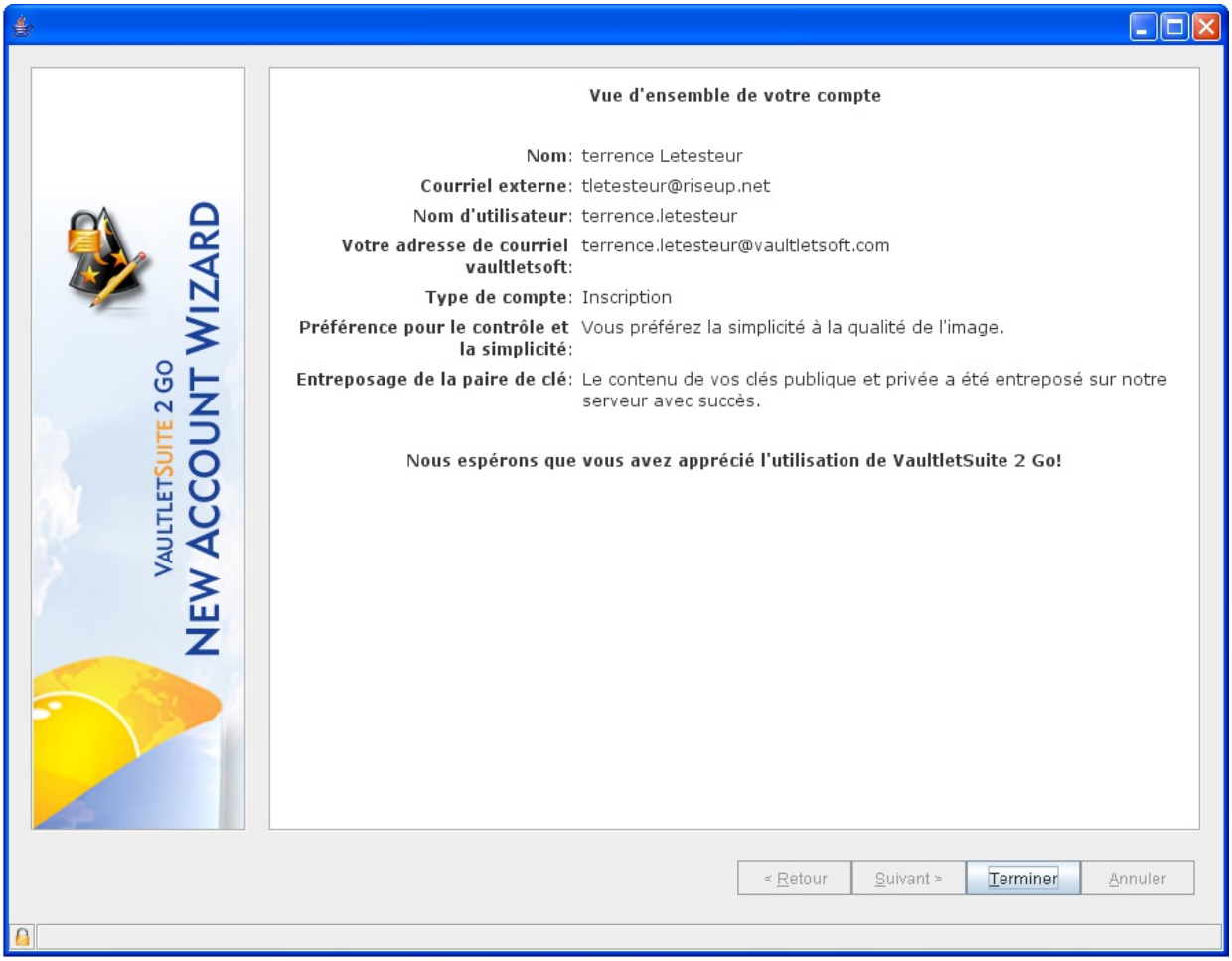

VAULTLETSUITE 2 GO
NEW ACCOUNT WIZARD
Vue d'ensemble de votre compte
Nom: terrence Letesteur
Courriel externe: tletesteur@riseup.net
Nom d'utilisateur: terrence.letesteur
Votre adresse de courriel vaultletsoft: terrence.letesteur@vaultletsoft.com
Type de compte: Inscription
Préférence pour le contrôle et la simplicité: Vous préférez la simplicité à la qualité de l'image.
Entreposage de la paire de clé: Le contenu de vos clés publique et privée a été entreposé sur notre serveur avec succès.
Nous espérons que vous avez apprécié l'utilisation de VaultletSuite 2 Go!
< Retour
Suivant >
Terminer
Annuler

Figure 16 : Nouvau compte VaultletSuite 2 Go

Première étape. **Cliquez** sur : Terminer pour finaliser la procédure de création du compte.

Félicitations, vous venez d'enregistrer un compte de courrier électronique VS2Go. Il est possible qu'une fenêtre apparaisse à ce moment pour vous présenter un *Message Système VS2Go* décrivant quelques unes des nouvelles fonctions du logiciel.

Cliquez sur : Fermer pour continuer. Il est conseillé d'installer toutes les mises à jour proposées.

2.3 Sur l'actualisation de VS2Go

Lorsque vous lancez VS2Go, il est possible que l'on vous demande d'actualiser le logiciel avec la plus récente mise à jour de VS2Go. Les mises à jour mineures sont optionnelles mais les mises à jour majeures du programme doivent être installées avant que vous puissiez continuer à vous servir du programme. Ces mises à jour comprennent d'importantes corrections de sécurité et autres améliorations.

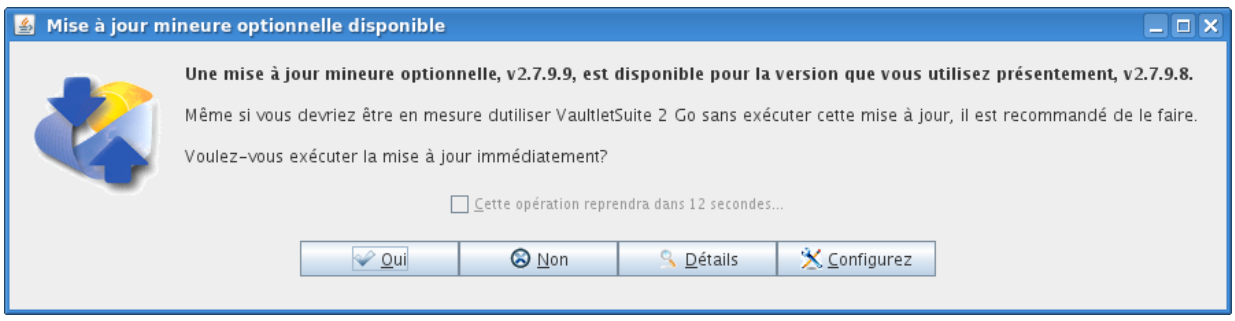

Mise à jour mineure optionnelle disponible
Une mise à jour mineure optionnelle, v2.7.9.9, est disponible pour la version que vous utilisez présentement, v2.7.9.8.
Même si vous devriez être en mesure dutiliser VaultletSuite 2 Go sans exécuter cette mise à jour, il est recommandé de le faire.
Voulez-vous exécuter la mise à jour immédiatement?
Cette opération reprendra dans 12 secondes...
Oui
Non
Détails
Configurez

Figure 17 : La fenêtre d'alerte de mises à jours mineures optionnelles

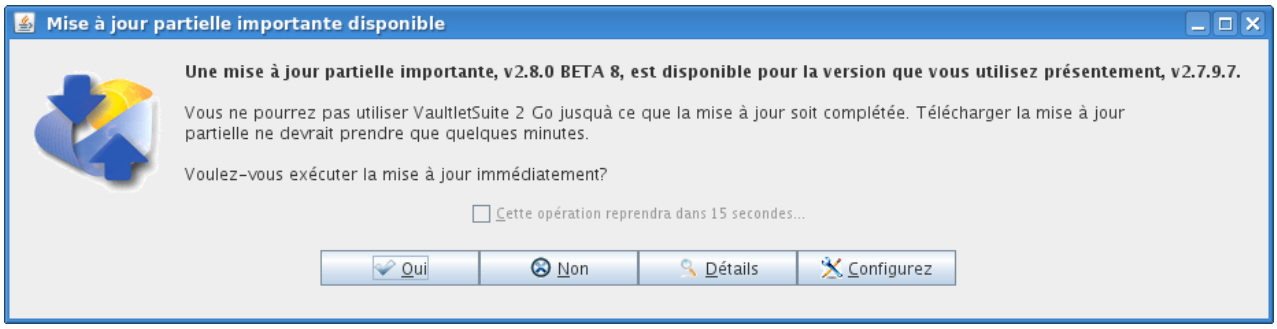

Mise à jour partielle importante disponible
Une mise à jour partielle importante, v2.8.0 BETA 8, est disponible pour la version que vous utilisez présentement, v2.7.9.7.
Vous ne pourrez pas utiliser VaultletSuite 2 Go jusquà ce que la mise à jour soit complétée. Télécharger la mise à jour partielle ne devrait prendre que quelques minutes.
Voulez-vous exécuter la mise à jour immédiatement?
Cette opération reprendra dans 15 secondes...
Oui
Non
Détails
Configurez

Figure 18 : La fenêtre d'alerte de mises à jours majeures partielles

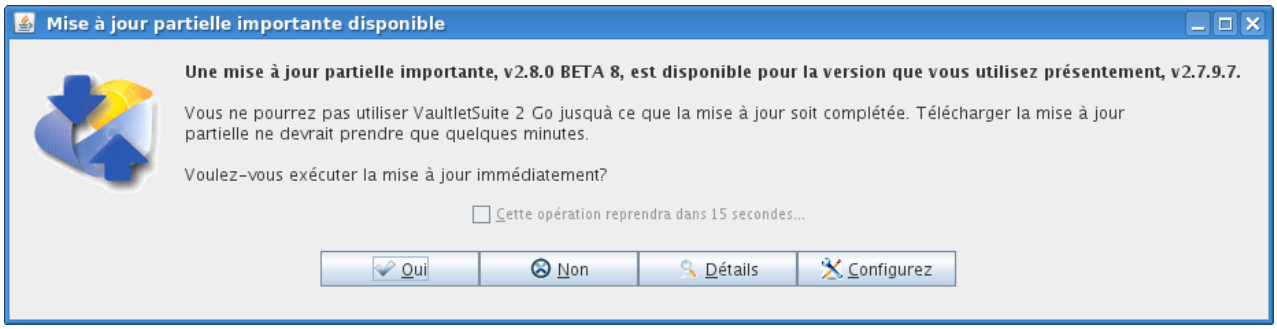

Mise à jour partielle importante disponible
Une mise à jour partielle importante, v2.8.0 BETA 8, est disponible pour la version que vous utilisez présentement, v2.7.9.7.
Vous ne pourrez pas utiliser VaultletSuite 2 Go jusquà ce que la mise à jour soit complétée. Télécharger la mise à jour partielle ne devrait prendre que quelques minutes.
Voulez-vous exécuter la mise à jour immédiatement?
Cette opération reprendra dans 15 secondes...
Oui
Non
Détails
Configurez

Figure 19: La fenêtre d'alerte de mise à jour majeure partielle supplémentaire

Les mises à jour seront automatiquement téléchargées et installées sur votre ordinateur ou votre unité de stockage amovible.

Comment utiliser VS2Go

Maintenant que vous avez enregistré un compte, vous pouvez commencer à utiliser l'un des systèmes de courrier électronique les plus sûrs disponibles sur Internet actuellement! Après l'enregistrement (ou après vous être dûment connecté), vous serez dirigé vers l'interface de gestion du courriel.

Première étape. **Cliquez sur** : ou **sélectionnez : Démarrer > Programmes > VaultletSuite2Go > VaultletSuite2Go** pour activer la console principale de *VaultletSuite 2 Go* et la fenêtre de connexion.

Figure 20 : La fenêtre Bienvenue à VaultletSuite 2 Go! [@vaultletsoft.com]

Commentaire : Si vous avez changé d'ordinateur depuis la dernière fois que vous avez accédé à votre compte, VS2Go vous interrogera sur l'emplacement de vos archives et de vos données VauletSoft. Les premières fois que vous vous connecterez, une fenêtre s'activera pour vous informer des nouvelles fonctions de VS2Go.

La fenêtre de la corbeille d'arrivée de VaultletMail apparaîtra alors.

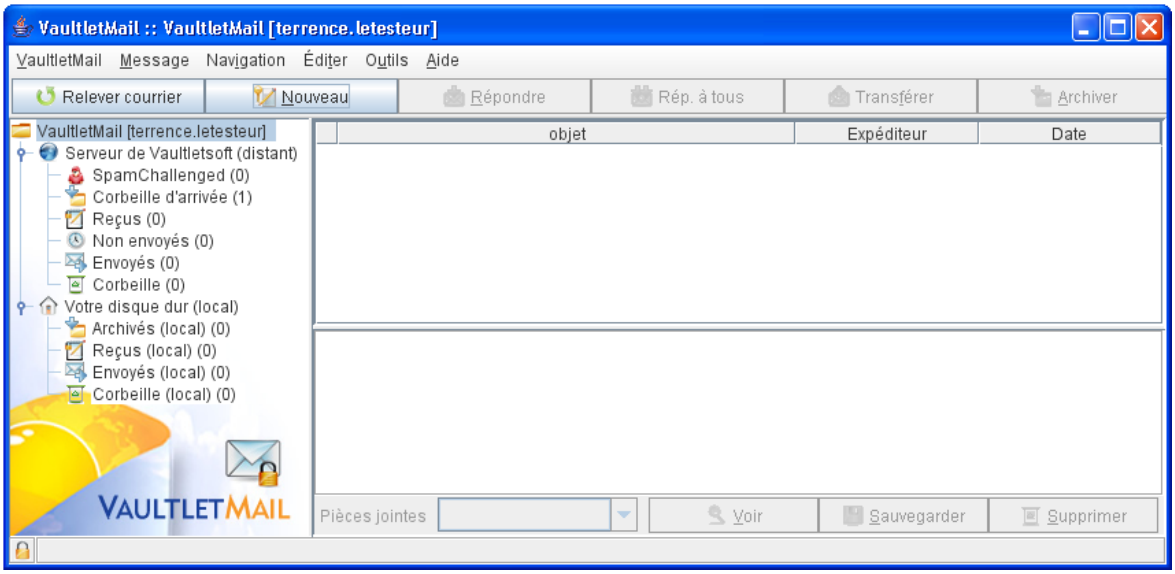


Figure 21 : La fenêtre de la corbeille d'arrivée de VaultletSuite 2

Remarquez que la console principale de VaultletSuite 2 Go, qui vous permet de naviguer entre le programme de courriel, l'outil de stockage de fichiers et l'outil de gestion de mots de passe de VaultletSuite, est toujours activée.

Figure 22 : La console principale de VaultletSuite 2 Go

3.1 Comment utiliser les fonctions principales de VS2Go

En fait, VS2Go fonctionne comme n'importe quel autre client de messagerie. Vous rédigez un message, choisissez des destinataires et leur envoyez le message. Cependant, VS2Go offre un éventail de fonctions de sécurité avancées que la plupart des autres programmes de courriel n'ont pas. Dans cette section, vous apprendrez à rédiger des messages et à gérer vos archives de courriel et vos fichiers.

Pour rédiger un nouveau message :

Première étape. **Cliquez** sur : pour ouvrir une fenêtre de *Nouveau message*.

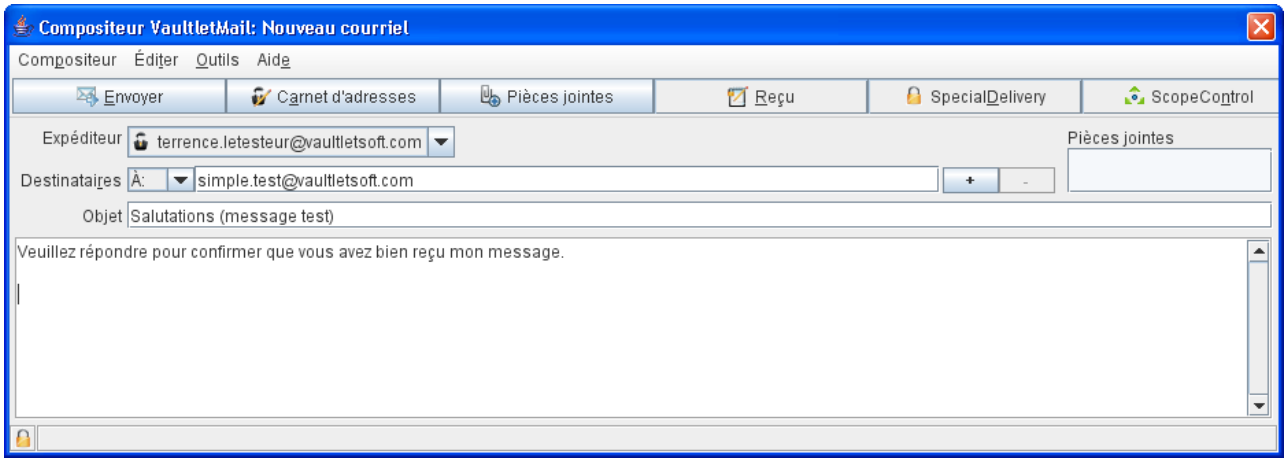


Figure 23. La fenêtre VaultletMail: nouveau message

Commentaire : Il est conseillé d'agrandir la fenêtre de *Rédaction* afin d'afficher toutes les fonctions du menu.

Deuxième étape. **Rédigez** votre message, saisissez l'adresse du destinataire et **cliquez** sur : lorsque vous avez terminé.

VaultletMail chiffrera automatiquement tous les messages envoyés à d'autres destinataires VS2Go (qui disposent d'une adresse @vaultletsoft.com). La prochaine section donne des directives concernant le chiffrement de messages envoyés à des destinataires qui n'ont pas de compte VaultletSoft.

Pour transférer des messages dans l'archive :

La liste des dossiers qui se trouve à gauche de la fenêtre principale de votre *corbeille d'arrivée* est divisée en trois catégories : *Serveur de Vaultletsoft (distant)* et *Votre disque dur (local)*, tel qu'illustré à la *Figure 21*. Tous les nouveaux messages, envoyés et reçus, sont initialement conservés sur un serveur de Vaultletsoft. Ce dernier offre un espace limité et un temps limité

de stockage. Effectuez régulièrement le transfert de vos messages vers votre ordinateur ou votre dispositif de stockage amovible (là où vous avez choisi de stocker vos archives à la section 2, ci-dessus). Votre compte local peut être aussi volumineux que votre ordinateur ou votre dispositif de stockage le permet. Tous vos messages seront stockés par l'entremise du chiffrement sécurisé VS2Go.

Première étape. **Sélectionnez** le(s) message(s) que vous souhaitez archiver.

Deuxième étape. **Sélectionnez : Message > Archiver** dans la barre de menus.

N'oubliez pas que si vous avez choisi l'option *Itinérant* pour transporter vos archives avec vous sur un dispositif amovible, vous devrez avoir ce dispositif avec vous en tout temps pour accéder à vos messages archivés. Vous pouvez toutefois recevoir et rédiger de nouveaux messages sans passer par votre dispositif amovible.

3.2 Comment utiliser VaultletFiler

VS2Go offre un service sécurisé de stockage de fichiers et utilise l'archive (que vous avez créé sur votre ordinateur ou sur votre clé USB) à cette fin. Vous pouvez transférer plusieurs fichiers que vous souhaitez protéger à l'aide du chiffrement VS2Go, et y accéder à partir de votre ordinateur ou dispositif de stockage amovible. Gardez à l'esprit que les fichiers qui se trouvent sur votre ordinateur seront transférés et chiffrés par VS2Go. Vous ne pourrez y accéder que si vous êtes connecté à Internet et à votre compte (les prochaines versions de Vaultletsoft intégreront une fonction d'accès hors ligne). Le VaultletFiler est accessible par la console principale deVaultletSuite 2 Go.

Première étape. **Sélectionnez : VaultletSuite 2 Go > VaultletFiler** pour ouvrir la fenêtre *VaultletFiler*

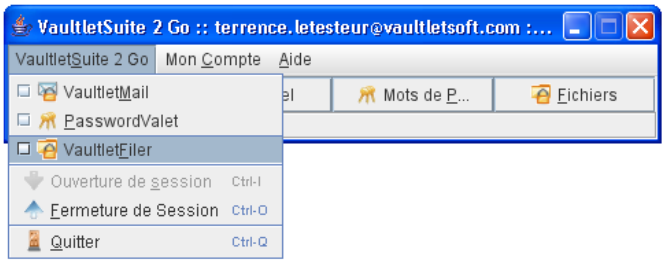


Figure 24. Sélectionner VaultletFiler par la console principale de VaultletSuite 2 Go

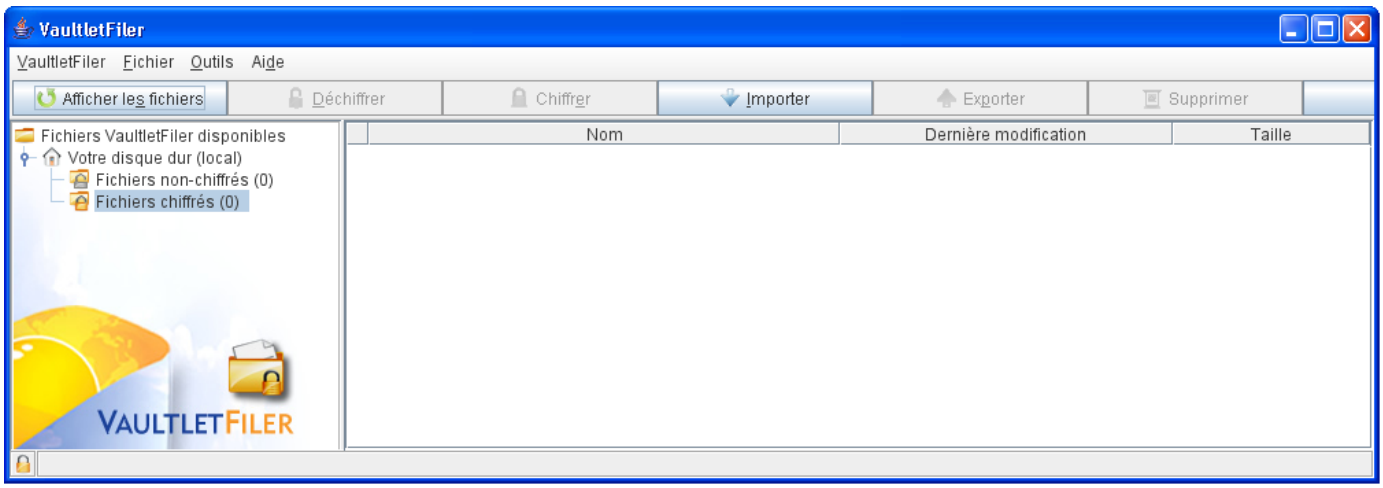


Figure 25. La fenêtre VaultletFiler

Pour importer (ou transférer) des documents dans le *VaultletFiler?*, suivez les étapes énumérées ci-dessous :

Deuxième étape. **Cliquez** sur :

Troisième étape. **Sélectionnez** le(s) fichier(s) à importer.

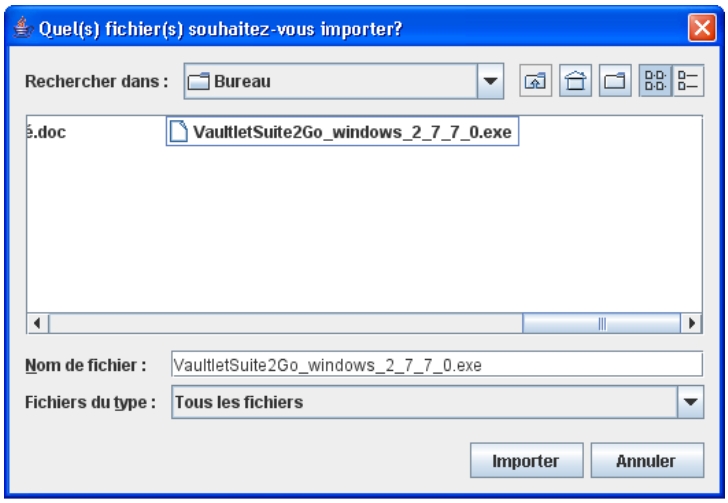


Figure 26. La fenêtre Quel(s) fichier(s) souhaitez-vous importer?

Quatrième étape. **Cliquez** sur : *Importer*

Le fichier apparaît maintenant dans la fenêtre *Fichiers chiffrés* :

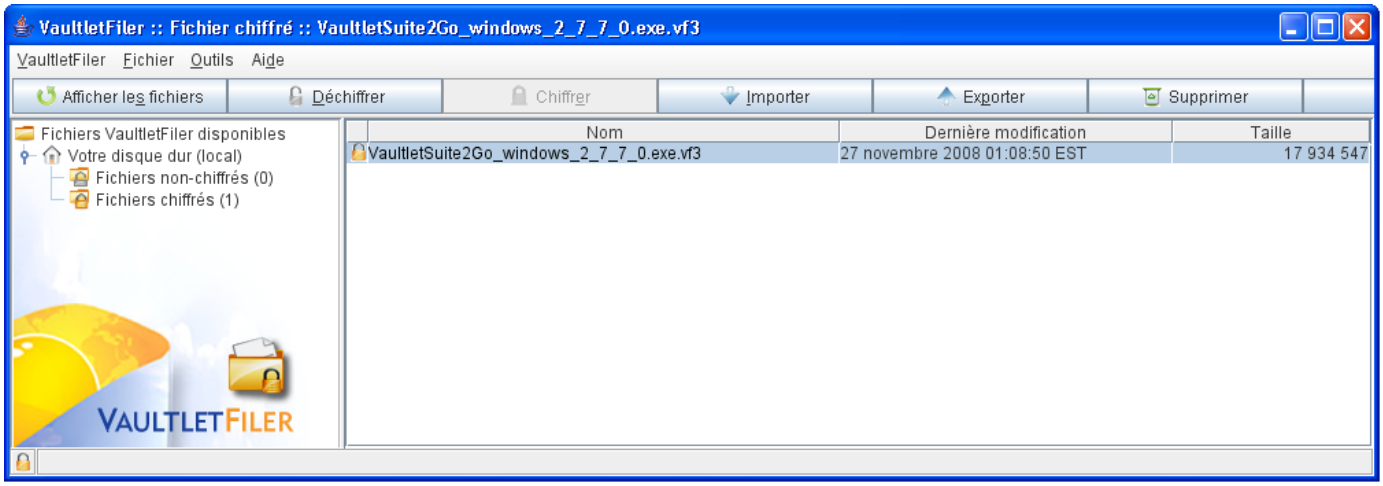


Figure 27. Les fichiers chiffrés affichés dans le VaultletFiler

Pour accéder à ce(s) fichier(s) ultérieurement, vous devrez d'abord le(s) exporter et le(s) déchiffrer. Pour ce faire, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez** le fichier à exporter dans la fenêtre *Fichiers chiffrés*.

Deuxième étape. **Cliquez** sur :

Troisième étape. **Choisissez** l'emplacement où les fichiers doivent être exportés.

On vous demandera alors si vous souhaitez d'abord déchiffrer le fichier. Si vous voulez y accéder (c.-à-d. le modifier ou l'activer), vous devrez déchiffrer le fichier.

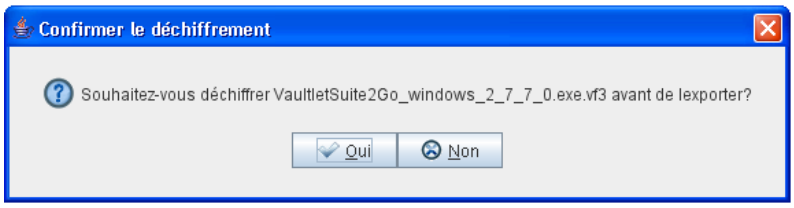


Figure 28: La Fenêtre Confirmer le déchiffrement

Quatrième étape. **Cliquez** sur *Oui* pour déchiffrer et exporter le(s) fichier(s) sélectionné(s) vers l'emplacement souhaité.

Fonctions avancées VaultletMail

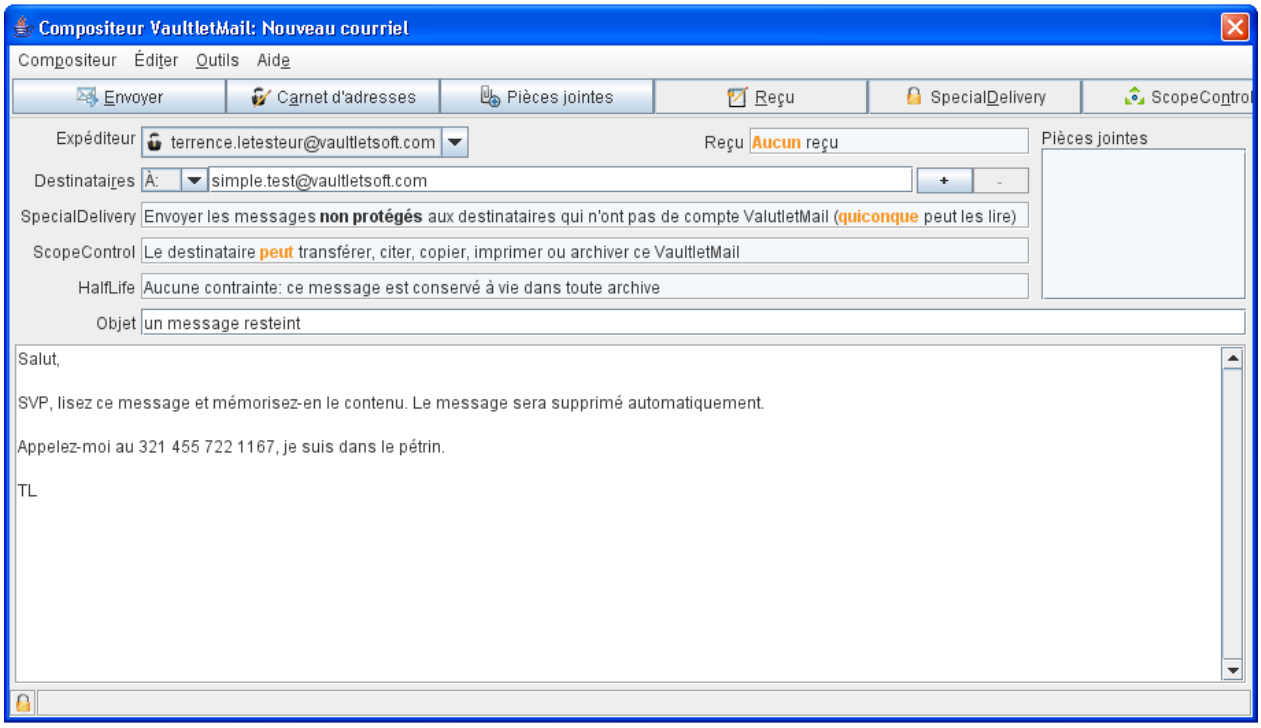
VS2Go comporte quelques fonctions supplémentaires qui augmentent encore le niveau de sécurité de vos communications par courrier électronique. Vous devez avoir choisi un *Compte bleu* lors de l'enregistrement pour profiter pleinement de ces fonctions.

- **Half-Life** – Vous permet de déterminer la durée de vie d'un message à partir du moment où le destinataire l'a ouvert. Vous pouvez préciser d'avance le nombre de fois que le message pourra être lu, ou déterminer une limite de temps avant que le message ne soit automatiquement supprimé. Cette fonction est utile pour envoyer des renseignements

sensibles qui ne doivent plus être accessibles après une période de temps donnée.

- **ScopeControl** – Vous permet de restreindre la capacité de votre destinataire à transférer votre message à une tierce partie ou de copier le contenu affiché dans la fenêtre principale du message original. Cela est utile pour empêcher qu'un destinataire commette accidentellement une 'fuite' des renseignements qui se trouvent dans votre message.
- **SpecialDelivery** – Vous permet d'envoyer des messages chiffrés, et d'utiliser les fonctions *Half-Life* et *Scope Control* si nécessaire, à l'extérieur du domaine VaultletSoft. Cela signifie que vous pouvez maintenir votre confidentialité lorsque vous communiquez avec des personnes qui utilisent d'autres services de messagerie (même des services non sécurisés).

Pour vérifier si ces fonctions complémentaires sont activées, **cliquez** sur : dans la fenêtre de *Rédaction de message VaultletMail* .


Compositeur VaultletMail: Nouveau courriel
Compositeur Éditer Outils Aide
Envoyer
Carnet d'adresses
Pièces jointes
Reçu
SpecialDelivery
ScopeControl
Expéditeur
terrence.letesteur@vaultletsoft.com
Reçu Aucun reçu
Pièces jointes
Destinataires À:
simple.test@vaultletsoft.com
SpecialDelivery Envoyer les messages non protégés aux destinataires qui n'ont pas de compte VaultletMail (quiconque peut les lire)
ScopeControl Le destinataire peut transférer, citer, copier, imprimer ou archiver ce VaultletMail
HalfLife Aucune contrainte: ce message est conservé à vie dans toute archive
Objet un message resteint
Salut,
SVP, lisez ce message et mémorisez-en le contenu. Le message sera supprimé automatiquement.
Appelez-moi au 321 455 722 1167, je suis dans le pétrin.
TL

Commentaire : Il est possible que vous deviez étirer la fenêtre pour afficher cet icône.

4.1 La fonction Half-Life

Il est possible de limiter la durée de vie d'un message, à partir du moment que ce dernier est arrivé dans la corbeille d'arrivée du destinataire. Pour ce faire, il suffit de **cliquer** sur le bouton *HalfLife* dans la barre de menus de la fenêtre de rédaction de message de *VaultletMail*.

Première étape. **Cliquez** sur : pour activer la fonction *Half-Life*.

Deuxième étape. **Sélectionnez** la durée de vie souhaitée pour le message (c.-à-d. la limite de temps que le message sera affiché avant d'être automatiquement supprimé, ou le nombre limite de fois que le message peut être ouvert, ou une combinaison des deux).

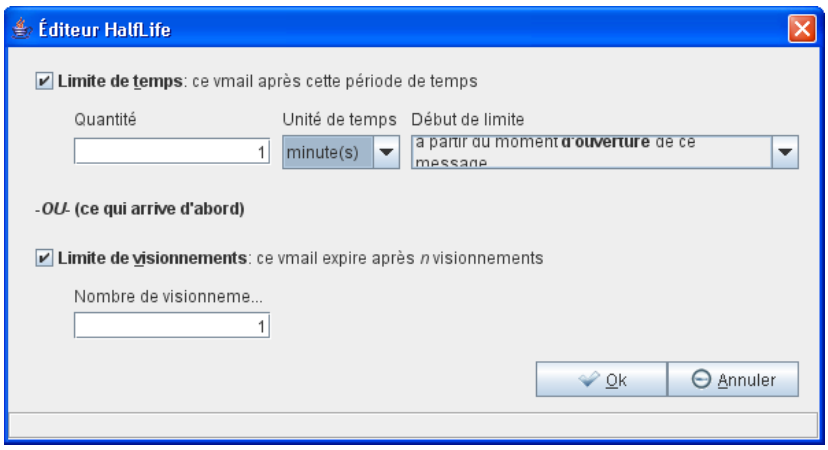


Figure 29. La fenêtre de la fonctionHalfLife

Troisième étape. **Cliquez** sur: lorsque vos réglages sont terminés.

Commentaire : La description de la fonction *HalfLife*, au dessus de votre message, devrait maintenant tenir compte des nouveaux réglages.

Figure 30 : La description de la fonction HalfLife

Quatrième étape. **Rédigez** votre message et **cliquez** sur :

Le destinataire recevra alors votre message. Il pourra voir les restrictions que vous avez imposées, tel qu'illustré ci-dessous :

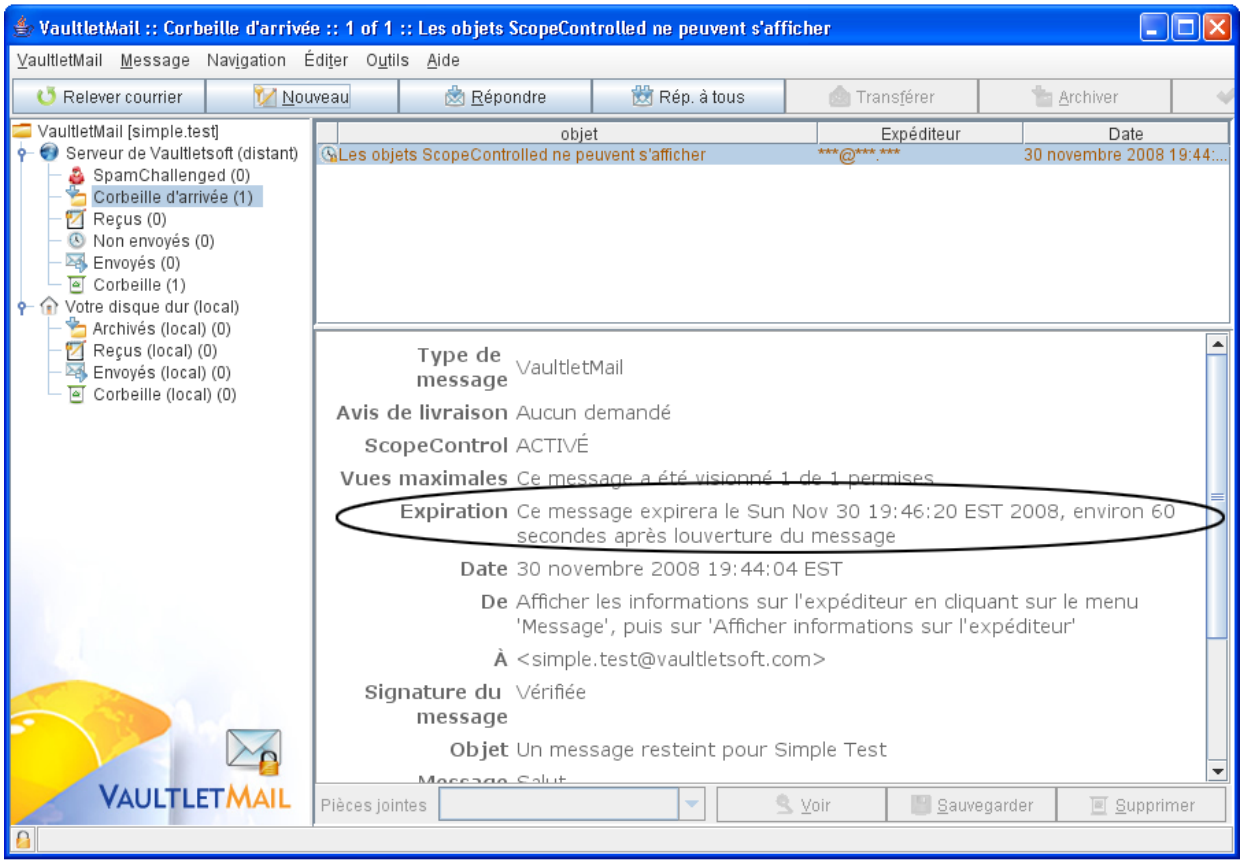
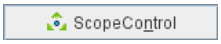


Figure 31. La corbeille d'arrivéeVaultletMail de votre destinataire affichant le message que vous avez envoyé et sa durée de vie

Quand la durée de vie du message sera révolue, ou quand la limite du nombre de fois où le message peut être affiché sera atteinte, le message sera automatiquement supprimé.

4.2 La fonction Scope Control

Vous pouvez empêcher vos destinataires de transférer votre message à une tierce partie ou de copier le contenu de votre message. Cela peut s'avérer utile pour empêcher que des 'accidents' se produisent et que votre message circule sur des listes électroniques.

Première étape. **Cliquez** sur : 

dans la fenêtre de rédaction de message *VaultletMail*.

Remarquez que la description de la fonction *Scope Control*, au dessus de votre message, est maintenant quelque peu modifiée :

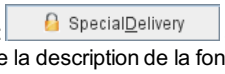
Figure 32 : La description de la fonction Scope Control

Il est maintenant impossible à vos destinataires de transférer votre message ou d'en copier, archiver ou imprimer le contenu.

4.3 La fonction SpecialDelivery

La fonction SpecialDelivery apporte la sécurité et la fonctionnalité de VS2Go à tous les utilisateurs de courrier électronique. Elle permet d'envoyer des messages chiffrés à n'importe quelle adresse de courriel (et d'utiliser HalfLife? et Scope Control si nécessaire). Cela peut paraître une tâche impossible, mais le truc est simple : il s'agit d'envoyer le message chiffré et d'inclure un lien vers un visualiseur sécurisé de SpecialDelivery, situé sur le site Internet de VaultletSoft?, qui permet d'afficher le message de façon sécurisée.

Commentaire : Initialement, cette approche peut sembler laborieuse à vos correspondants. Par contre, lorsque ceux-ci auront complété le processus une première fois, tous les échanges subséquents seront considérablement plus rapides. Vous devez vous rappeler que si vous et vos correspondants voulez éviter que ces derniers soient en danger en utilisant un service de courriel non sécurisé, alors il est judicieux de prendre cette mesure de sécurité supplémentaire.

Première étape. **Cliquez** sur : 

après avoir saisi une adresse de courriel externe dans le champ *Destinataires:*. Remarquez que la description de la fonction *Special Delivery*, au dessus de votre message, est maintenant quelque peu modifiée :

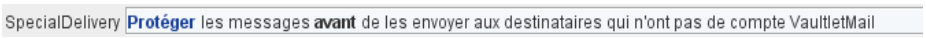


Figure 33 : La description de la fonction Special Delivery

Vous pouvez maintenant activer les fonctions *HalfLife* et *Scope Control*, si nécessaire.

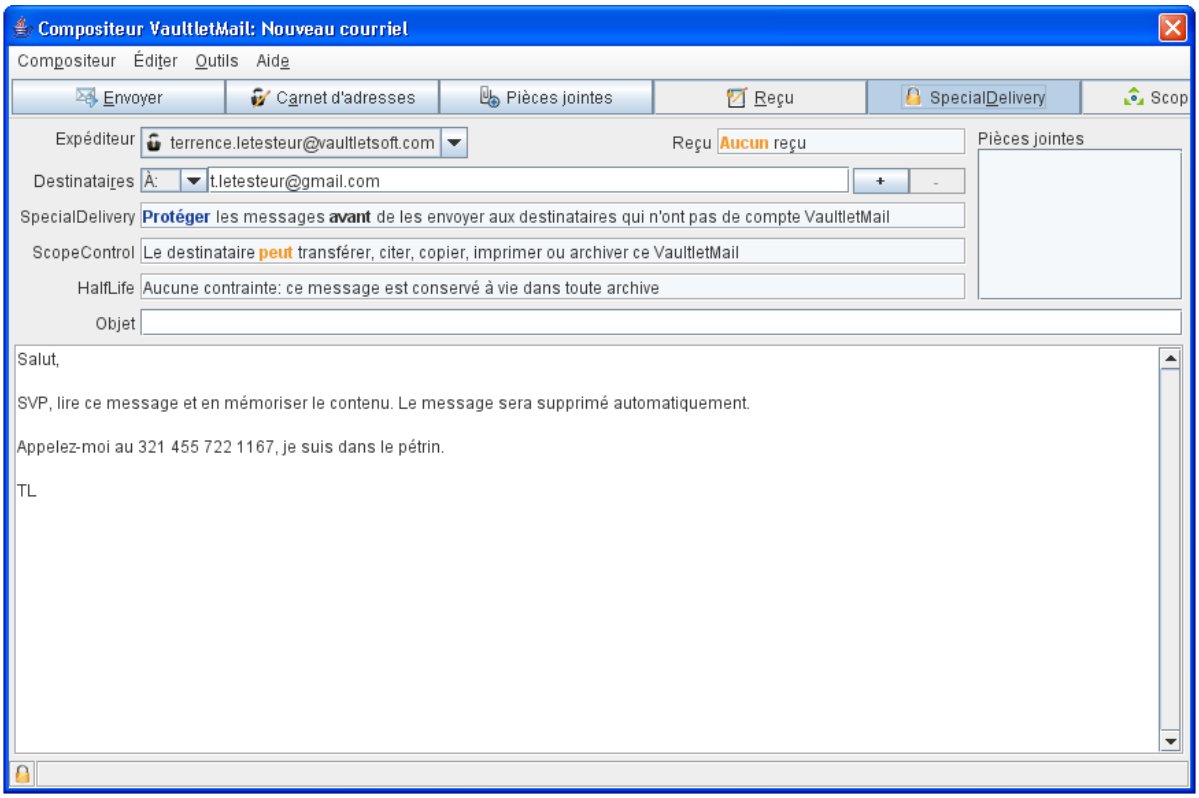


Figure 34: La fenêtre de rédaction de nouveau messageVaultletMail

Deuxième étape. **Rédigez** votre message et **envoyez-le**.

On vous demandera de créer un code secret, que votre destinataire devra **saisir à l'identique** lorsque cela lui sera demandé par le système VS2Go. Cette opération sert à authentifier l'identité des deux parties en communication.

Troisième étape. **Saisissez** un code secret (d'au moins 8 caractères) et **cliquez** sur :

.

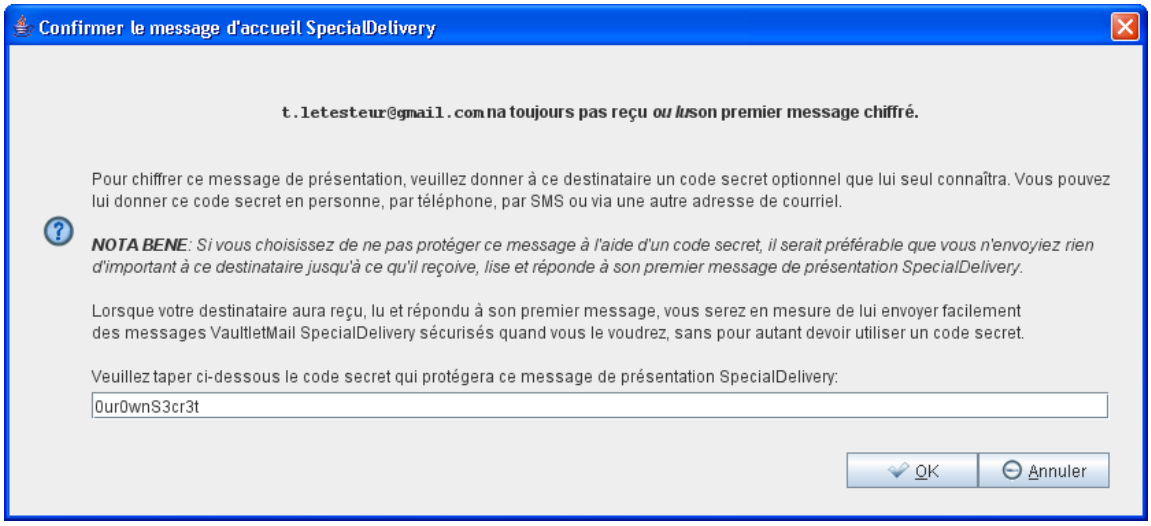

Confirmer le message d'accueil SpecialDelivery
t.letesteur@gmail.com n'a toujours pas reçu ou lu son premier message chiffré.
Pour chiffrer ce message de présentation, veuillez donner à ce destinataire un code secret optionnel que lui seul connaîtra. Vous pouvez lui donner ce code secret en personne, par téléphone, par SMS ou via une autre adresse de courriel.
NOTA BENE: Si vous choisissez de ne pas protéger ce message à l'aide d'un code secret, il serait préférable que vous n'envoyiez rien d'important à ce destinataire jusqu'à ce qu'il reçoive, lise et réponde à son premier message de présentation SpecialDelivery.
Lorsque votre destinataire aura reçu, lu et répondu à son premier message, vous serez en mesure de lui envoyer facilement des messages VaultletMail SpecialDelivery sécurisés quand vous le voudrez, sans pour autant devoir utiliser un code secret.
Veuillez taper ci-dessous le code secret qui protégera ce message de présentation SpecialDelivery:
0ur0wnS3cr3t
OK
Annuler

Figure 35 : La fenêtre Confirmer le message d'accueil SpecialDelivery

Passez le code secret à votre correspondant par SMS, en personne ou par téléphone. N'oubliez pas que cette opération d'authentification ne doit être effectuée qu'une seule fois pour chaque nouveau destinataire.

Directives à l'intention du destinataire

Vous recevrez le messageVaultletSoft dans votre programme de messagerie normal.

Objet: VaultletMail SpecialDelivery: un message restreint
De: "terrence Letesteur" <terrence.letesteur@vaultletsoft.com>
Date: Dim 30 novembre 2008 19:31
À: tletesteur@riseup.net
Priorité : Normale
Options: Afficher l'en-tête complet | Voir la version imprimante | Télécharger en tant que fichier | Ajout

```
Hi,

I'm sending you a secret and secure VaultletMail SpecialDelivery message that nobody
else can read.

To read the secure contents of this secret message, hit "Cntl + A" (select all) on
your keyboard, followed by "Cntl + C" (copy).

Once you've done that, click on this link to view it:
https://www.vaultletsoft.com/start/specialdelivery-applet.html

Best,

terrence

--
p.s.: To find out more about VaultletMail SpecialDelivery messages, go here:
https://www.vaultletsoft.com/products/specialdelivery.html
```

Figure 36 : Un messageSpecialDelivery de VaultletSoft

Première étape. **Suivez** les directives incluses dans le message, en **copiant** le contenu au complet. **Cliquez** sur le lien pour ouvrir un nouvelle fenêtre de navigateur.

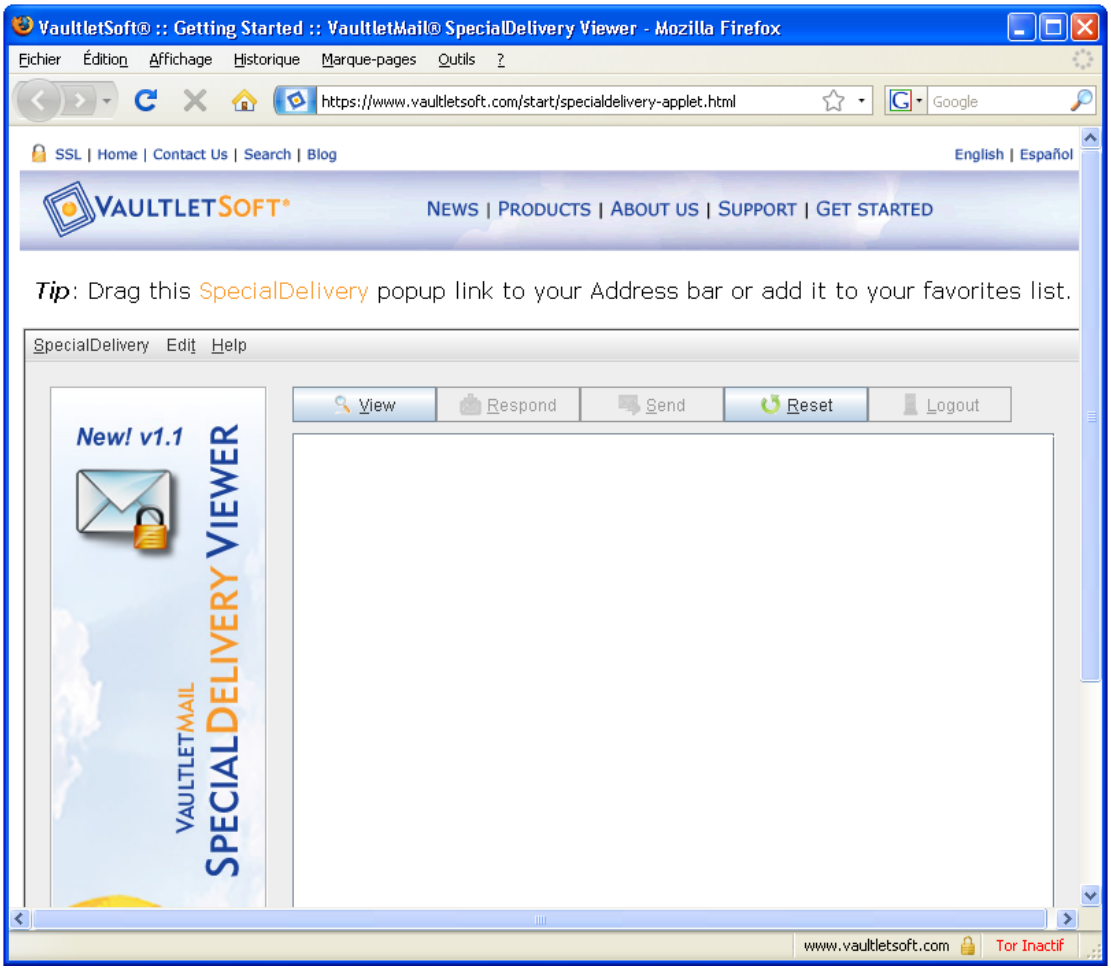


Figure 37. Le message SpecialDelivery de VaultletSoft Message affiché dans un compte de courriel non-VaultletSoft

Lorsque la page sera chargée, on vous demandera d'installer l'application Java depuis le site de VaultletSoft Inc. Il s'agit d'un petit programme qui effectuera le chiffrement et le déchiffrement des messages VaultletSoft sur votre ordinateur. Il est possible que l'on vous demande si vous souhaitez 'Toujours faire confiance à cet éditeur'. Prenez votre décision en fonction de si vous voulez ou non répondre à cette question chaque fois que vous lancez le visualiseur SpecialDelivery.

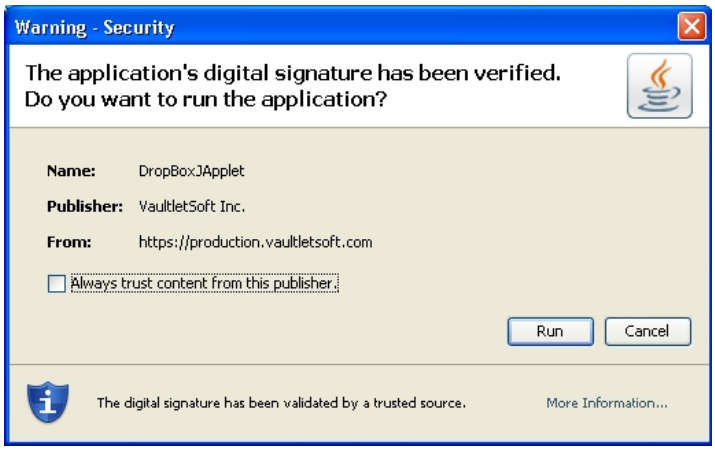

Warning - Security
The application's digital signature has been verified.
Do you want to run the application?
Name: DropBoxJApplet
Publisher: VaultletSoft Inc.
From: https://production.vaultletsoft.com
Always trust content from this publisher.
Run
Cancel
The digital signature has been validated by a trusted source.
More Information...

Figure 38 : La fenêtre d'alerte de sécurité

Deuxième étape. **Cliquez** sur *Run*.

Lorsque l'installation est terminée, **faites Ctrl+V** pour coller le contenu du courriel dans la fenêtre appropriée (si cela ne s'est pas produit automatiquement).

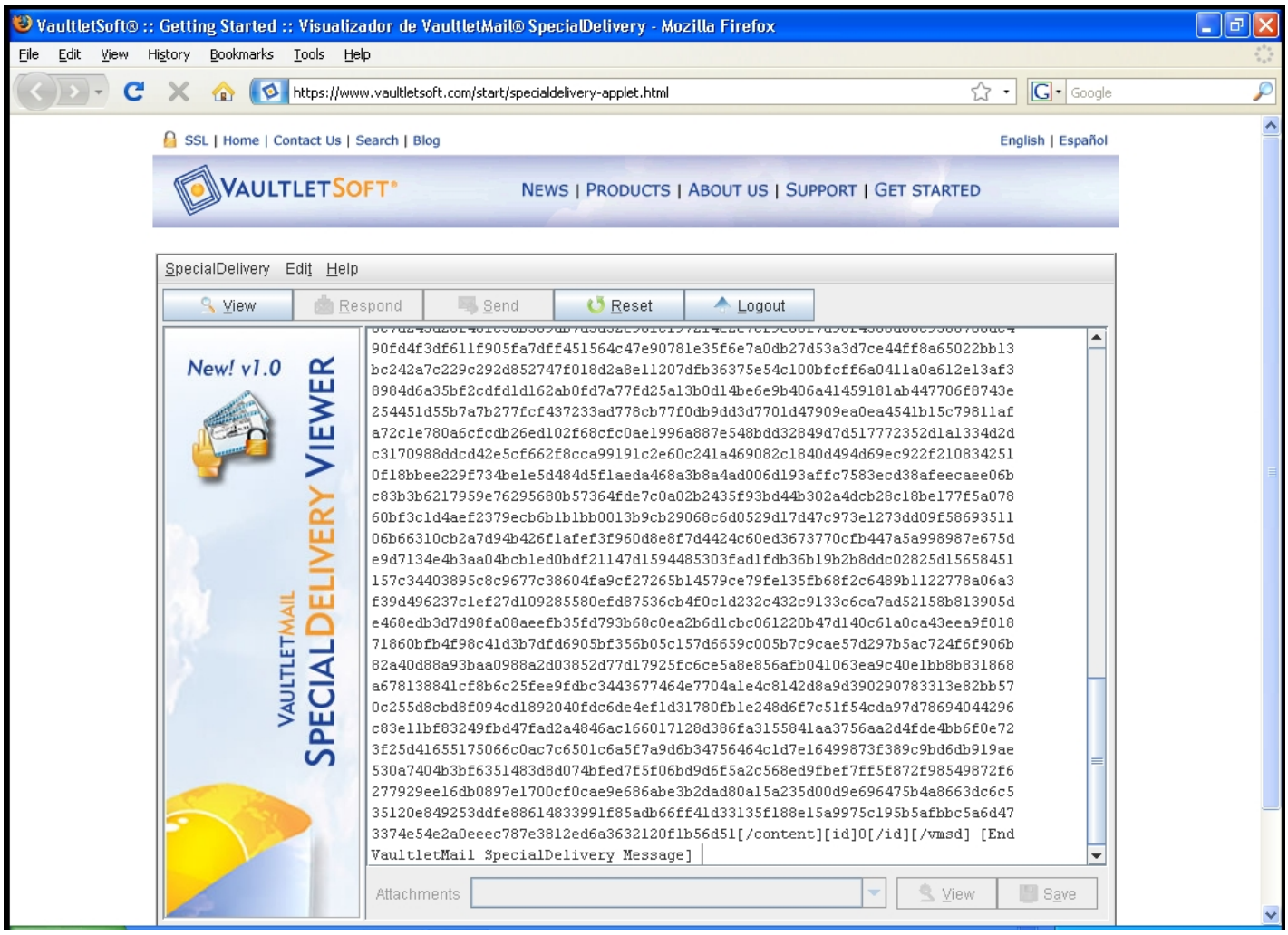


Figure 39 : La fenêtre Getting Started de VaultletSoft

Troisième étape. **Cliquez** sur : pour le déchiffrer.

Le système commencera à déchiffrer le message. On vous demandera de créer un compte VS2Go, afin d'envoyer et de recevoir des messages sécurisés de la part d'expéditeurs Vaultlet à l'avenir.

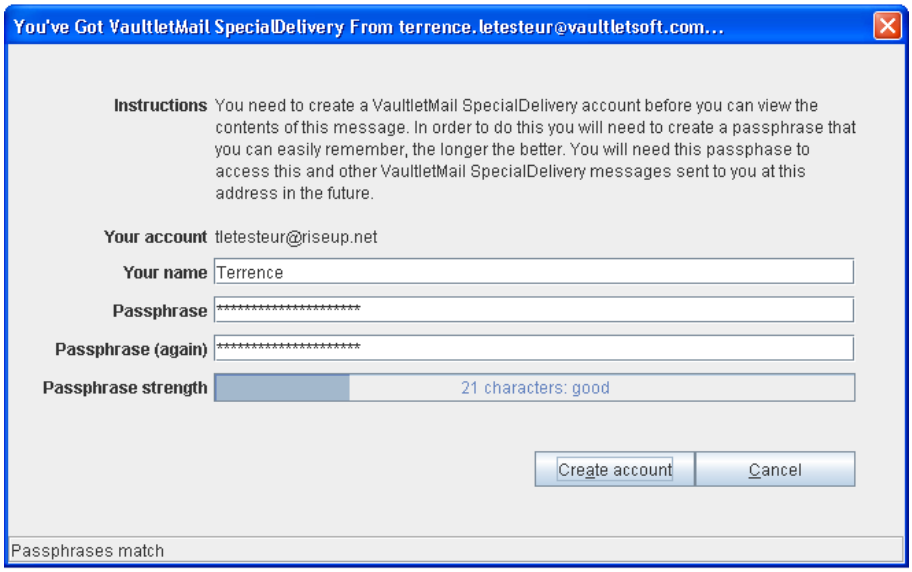

You've Got VaultletMail SpecialDelivery From terrence.letesteur@vaultletsoft.com...
Instructions
You need to create a VaultletMail SpecialDelivery account before you can view the contents of this message. In order to do this you will need to create a passphrase that you can easily remember, the longer the better. You will need this passphase to access this and other VaultletMail SpecialDelivery messages sent to you at this address in the future.
Your account
tletesteur@riseup.net
Your name
Terrence
Passphrase
Passphrase (again)
Passphrase strength
21 characters: good
Create account
Cancel
Passphrases match

Figure 40 : La fenêtre You've Got VaultletMail SpecialDelivery From ...

Quatrième étape. **Saisissez** le nom d'utilisateur et la phrase secrète de votre nouveau compte.

Commentaire : Vous ne créez pas un compte de **courriel** sur le serveur de VS2Go. Vous ne faites qu'enregistrer votre adresse de courriel actuelle de telle sorte que vous pourrez dorénavant communiquer de façon sécurisée avec des correspondants qui disposent d'un compte VS2Go.

Cinquième étape. **Cliquez** sur :

Sixième étape. **Acceptez** le Contrat d'utilisation pour continuer.

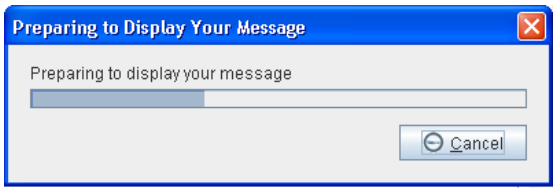


Figure 41 : La fenêtre Preparing to Display Your Message

La dernière étape consiste à confirmer le code secret créé par l'auteur du message pour le protéger.

Message Protected by Secret Code
The sender of this message has protected it with a secret code that only you should know.
Please type it in below.
0ur0wnS3cr3t
Okay
Cancel

Figure 42 : La fenêtre Message Protected by Secret Code

Septième étape. **Saisissez** le code secret pour afficher le message original :

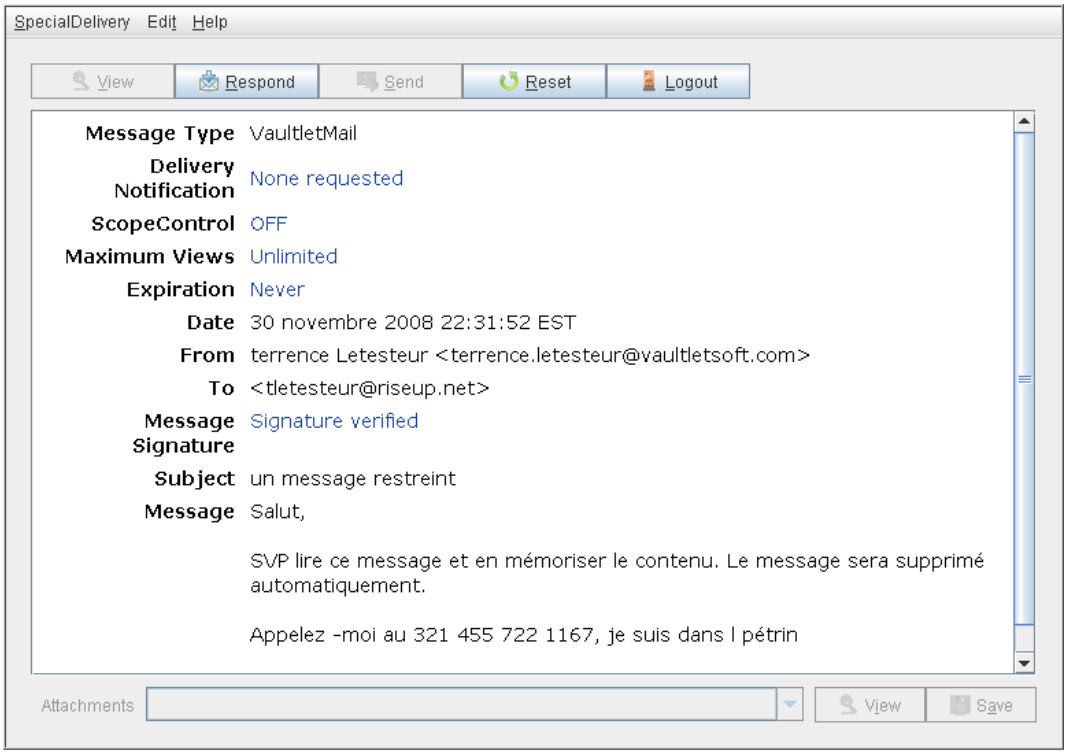


Figure 43 : L'affichage du message après avoir saisi le code secret

Vous pouvez désormais répondre au message de façon sécurisée en utilisant le bouton *Respond* sur cette même fenêtre. Toutes les communications subséquentes entre vous et ce correspondant seront beaucoup plus simples. Vous n'aurez qu'à ouvrir le lien inclus dans le message et à vous connecter avec les renseignements déjà créés. Vous n'aurez plus jamais à saisir de codes secrets suite à cette première opération.

Faq et questions récapitulatives

VS2Go comporte plusieurs autres fonctions qui ne sont pas abordées dans ce guide. Vous pouvez toujours vous référer à la VaultMail Tips Page (Page de conseils) et aux FAQs pour plus de renseignements.

Même si cet outil ne semble pas particulièrement simple de prime abord, le programme VaultletSuite 2 Go a été conçu et développé avec minutie pour être facile d'utilisation. Les développeurs travaillent constamment à améliorer l'interface et la fonctionnalité du programme. C'est l'un des seuls services de courrier électronique gratuits offrant une fonction de chiffrement des messages et fichiers. La capacité d'envoyer des messages chiffrés à l'extérieur du domaineVaultletSoft peut s'avérer fort importante dans le cadre d'une stratégie de communication sécurisée.

Claudia et Pablo ont passé une bonne partie de la journée à utiliser VS2Go. Ils ont réussi à se créer chacun un compte et ont pu échanger des messages chiffrés. Cependant, Pablo a encore quelques questions :

Q. : *Si je crée un compte pour utilisateurs itinérants et que je choisis la méthode Simplicité pour stocker ma clé privée, de quoi ai-je besoin pour accéder à mon compte à partir de n'importe quel ordinateur?*

R. : *Tu auras besoin de la phrase secrète du compte pour te connecter et voir tes messages qui sont stockés sur le serveur de VaultletSoft. Si tu souhaites accéder à tes fichiers et archives, alors tu auras aussi besoin de ta clé USB.*

Q. : *Que se passe-t-il si j'oublie ou perds l'un ou l'autre de mes mots de passe pour accéder au compte?*

R. : *Cela pose un problème, parce que la méthode de chiffrement VS2Go repose sur l'utilisation de la phrase secrète. Si tu demandes à ce que ta phrase secrète soit réinitialisée, tu perdras automatiquement l'accès à tous les messages et fichiers chiffrés envoyés et reçus préalablement, et stockés dans le VaultletFiler. Tu recevras un code de connexion temporaire à ton adresse de rechange, ce qui te permettra tout de même de continuer à utiliser ton adresse de courriel VaultletSoft. VS2Go générera alors une nouvelle paire de clés, à partir de ta nouvelle phrase secrète, que le système utilisera dorénavant pour chiffrer ton compte.*

Q. : *Je veux m'assurer qu'une adresse de courriel de rechange soit associée à mon compte. Peux-tu me rappeler ce que je dois faire?*

R. : *Tu n'as qu'à te connecter à ton compte et sélectionner l'option Voir l'information du compte, à partir du menu Mon compte.*

Q. : *Je suis encore un peu incertain quant à certaines options du processus d'enregistrement.*

R. : *Si tu n'es pas certain, essaie la procédure d'enregistrement Simplicité - Rapide et facile. Le programme stockera tes archives sur ton ordinateur et ta clé privée sur un serveur de VaultletSoft. Tout ce que tu as à faire est de ne pas oublier ta phrase secrète, et te rappeler que tu ne peux accéder à ton compte qu'à partir de cet ordinateur.*

Q. : *Mon compte Bleu est enregistré pour un an seulement. Que se passera-t-il à la fin de cette période?*

R. : *Il existe plusieurs moyens de prolonger la durée de vie d'un compte Bleu. Tu peux payer, bien sûr. Tu peux aussi demander à trois personnes de créer des comptes VS2Go en utilisant ton adresse de courriel comme référent. Sinon, tu peux aussi saisir un Code Promo, que tu pourras trouver dans la copie physique de NGO in a Box - Security Edition. Si tu*

sélectionnes l'option Voir l'information du compte, à partir du menu Mon compte, tu peux choisir celle de ces méthodes qui te convient le mieux. Par ailleurs, tu peux sélectionner l'option Contactez-nous, à partir du menu Aide, et écrire directement à VaultletSoft pour demander une prolongation de la durée de vie de ton compte.

Q. : *J'ai peur que mes correspondants soient réticents à passer par la procédure Special Delivery pour voir mes messages chiffrés.*

R. : *Tu as peut-être raison. Malheureusement la plupart des gens ont tendance à être moins préoccupés par les enjeux de sécurité qu'ils le devraient, et sont souvent réticents à acquérir de nouveaux outils. Certains de tes correspondants te demanderont peut-être de renvoyer tes messages en utilisant une méthode moins sûre. C'est à toi de déterminer si tu es prêt à mettre ta propre sécurité en danger. Sinon, tu devras convaincre tes correspondants que la confidentialité des communications est assez importante pour que l'on supporte des inconvénients mineurs. Évidemment, tu peux toujours les diriger vers le livret pratique de Security in-a-Box ou le manuel Digital Security and Privacy for Human Rights Defenders.*

Q. : *Disons que je reçois un message Special Delivery et que je suis capable de le déchiffrer à même mon navigateur Internet. Si je réponds à ce message, en cliquant sur le bouton Respond à partir de la même fenêtre, est-ce que la communication est toujours sécurisée?*

R. : *Oui. Le but de cette procédure (c.-à-d. télécharger et lancer cette application Java, créer un nom de compte et une phrase secrète, et ouvrir le message à partir d'un lien) est de conserver tous les éléments nécessaires à une communication chiffrée. Ta réponse, ainsi que tous les messages subséquents échangés par la fonction Special Delivery, seront sécurisés.*

5.1 Questions récapitulatives

- En quoi VS2Go est-il plus sûr qu'un compte de courriel normal?
- Quels sont les trois éléments que vous devez avoir avec vous (et sur votre ordinateur) pour être en mesure d'accéder à votre compte VS2Go?
- Comment pouvez-vous modifier des fichiers stockés dans le FileVault?
- Comment pouvez-vous transférer des messages à partir des serveurs VaultletSoft vers votre ordinateur ou votre dispositif de stockage amovible?
- Quelle est la différence entre HalfLife et Scope Control?
- Si vous avez envoyé un message avec des restrictions concernant la durée de vie ou le nombre limite d'affichages, que s'affiche-t-il dans l'en-tête de *l'Objet* lorsque votre destinataire reçoit le message?

Thunderbird - client de courriel sécurisé

Short Description:

Mozilla Thunderbird est un client de messagerie électronique gratuit, de source ouverte, qui permet de recevoir, envoyer et archiver vos courriels. Vous pouvez gérer plusieurs comptes de courrier électronique à l'aide d'un programme unique. **Enigmail** et **GnuPG** vous offrent des options supplémentaires, dont l'authentification, la signature numérique et le chiffrement de vos messages, ce qui accroît la confidentialité et la sécurité de vos communications par courrier électronique.

Online Installation Instructions:

Pour télécharger Thunderbird, Enigmail et GnuPG

- *Lisez la courte introduction aux* ***Guides pratiques*** [1]
- ***Cliquez*** *sur l'icone* ***Thunderbird*** *ci-dessous pour ouvrir la page Internet* ***www.mozilla.com/thunderbird***
- ***Cliquez*** *sur le lien* ***Téléchargement gratuit*** *pour sauvegarder le fichier d'installation sur votre ordinateur; localisez ensuite le fichier, puis* ***double-cliquez*** *dessus*
- ***Cliquez*** *sur l'icone* ***Enigmail*** *ci-dessous pour ouvrir la page* ***www.enigmail.mozdev.org/download***
- ***Cliquez à droite*** *sur le lien* ***Download v1.1.2 for Thunderbird 3.1*** *et sauvegardez le module complémentaire sur votre* ***Bureau***
- ***Cliquez*** *sur l'icone* ***GnuPG*** *ci-dessous pour ouvrir la page* ***www.gnupg.org/download***
- ***Faites dérouler*** *la page jusqu'à la section* ***Binaries****, puis* ***cliquez*** *sur le lien* ***FTP*** *associé à l'option GnuPG 1.4 compiled for Microsoft Windows, puis sauvegardez le fichier d'installation sur votre ordinateur*
- *Poursuivez la lecture de la* ***Section 4.1*** *de ce guide pratique* ***Thunderbird*** *pour installer* ***Enigmail*** *et* ***GnuPG***
- *Si vous avez sauvegardé les exécutables et les fichiers d'extension sur votre ordinateur, vous pouvez les supprimer après l'installation.*

Thunderbird: **Enigmail**: **GnuPG**:

[141] ENIGMAIL [142] GnuPG [143]

Site Internet

- **www.mozilla.com/thunderbird** [144]
- **www.enigmail.mozdev.org** [145]
- **www.gnupg.org** [146]

Configuration requise

- Compatible avec toutes les versions de Windows

Versions utilisées pour rédiger ce guide

- Thunderbird 3.1.5
- Enigmail 1.1.2
- GNU Privacy Guard (GnuPG) 2.0.4

Licence

- FLOSS (Free/Libre Open Source Software)

Lecture préalable

- Livret pratique Security in-a-box, chapitre **7. Préserver la confidentialité de vos communications sur Internet** [116]

Niveau: 1: Débutant, **2: Moyen** et **3: Intermédiaire**, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 40 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de gérer plusieurs comptes de courrier électronique à l'aide d'un seul et unique programme.
- La capacité de lire et composer des messages lorsque vous n'êtes pas connecté à Internet.
- La capacité d'utiliser le chiffrage par clé publique (asymétrique) pour faire en sorte que vos courriels restent confidentiels.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Le client de messagerie **Mozilla Thunderbird** est disponible pour **GNU Linux**, **Mac OS**, **Microsoft Windows** et d'autres systèmes d'exploitation. En ce qui a trait à la sécurité numérique, la gestion simultanée de plusieurs comptes de courrier électronique est une tâche complexe, c'est pourquoi il est *fortement recommandé* d'utiliser **Mozilla Thunderbird** à cette fin. Les avantages que présente **Thunderbird**, un client de messagerie *libre* et *gratuit*, multi plateforme et de *source ouverte*, sont d'autant plus importants lorsqu'on le compare à ses rivaux commerciaux comme **Microsoft Outlook**. Cela dit, si vous préférez utiliser un autre programme que **Mozilla Thunderbird**, nous recommandons les trois options suivantes, également gratuites et de source ouverte:

- **Claws Mail** [147] disponible pour **GNU Linux** et **Microsoft Windows**;
- **Sylpheed** [148] disponible pour **GNU Linux**, **Mac OS** et**Microsoft Windows**;
- **Alpine** [149] disponible pour **GNU Linux**, **Mac OS** et**Microsoft Windows**.

1.1 À propos de cet outil

Mozilla Thunderbird est un client de messagerie électronique libre, gratuit, multi plateforme et de source ouverte, qui permet de recevoir, envoyer, trier et archiver des messages de courrier électronique. Un client de messagerie est une application informatique qui vous permet de télécharger et gérer vos courriels sans utiliser un navigateur Internet. Vous pouvez gérer plusieurs comptes de courriel à l'aide sd'un seul et unique programme de messagerie. Vous devez avoir au moins un compte de courrier électronique pour utiliser **Thunderbird**. Vous pouvez également créer des comptes **Gmail** [150] ou **RiseUp** [151] si vous le souhaitez.

Enigmail est un module complémentaire conçu pour **Thunderbird**. Il donne accès aux fonctions d'authentification et de chiffrement offertes par **GNU Privacy Guard** (**GnuPG**).

GnuPG est un programme de chiffrement par clé publique (asymétrique) utilisé pour générer et gérer des paires de clés afin de chiffrer et déchiffrer des messages pour préserver la confidentialité et la sécurité de vos communications par courrier électronique. Comme nous le verrons plus loin dans ce chapitre, **GnuPG** doit être installé pour qu'**Enigmail** fonctionne.

Comment installer Thunderbird

Sommaire des sections de cette page:

- **2.0 Comment installer Thunderbird**
- **2.1 Comment désactiver l'option Recherche et indexation globales dans Thunderbird**
- **2.2 Comment enregistrer un compte de courrier électronique dans Thunderbird**
- **2.3 Comment enregistrer des comptes de Blogs, de nouvelles et de Groupes de discussion dans Thunderbird**

2.0 Comment installer Thunderbird

L'installation de **Thunderbird** est un processus relativement simple et rapide. Pour lancer l'installation de **Thunderbird**, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** sur Thunderbird Setup 3.1.7; il est possible que la boîte de dialogue de confirmation *Fichier ouvert - Avertissement de sécurité* s'affiche à ce moment. Si c'est le cas, **cliquez** sur Exécuter pour afficher la fenêtre suivante:

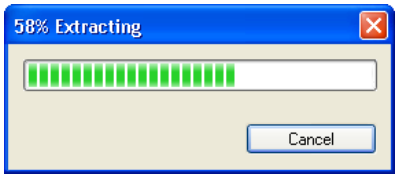


Figure 1: La barre de progression de l'extraction

Lorsque l'extraction des fichiers de **Thunderbird** est complétée, la fenêtre *Bienvenue dans l'assistant d'installation de Mozilla Thunderbird* apparaît.

Deuxième étape. **Cliquez** sur Suivant > pour activer la fenêtre *Mozilla Thunderbird - Type d'installation*.

Troisième étape. **Cliquez** sur Suivant > pour accepter les réglages par défaut et afficher la fenêtre suivante:

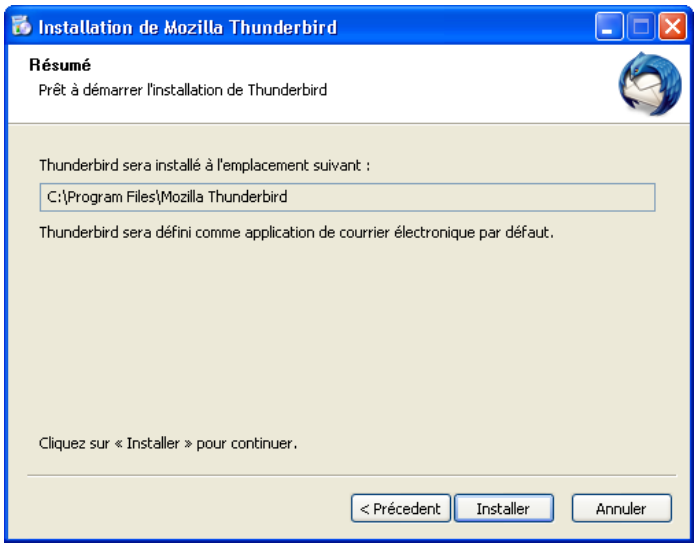

Installation de Mozilla Thunderbird
Résumé
Prêt à démarrer l'installation de Thunderbird
Thunderbird sera installé à l'emplacement suivant :
C:\Program Files\Mozilla Thunderbird
Thunderbird sera défini comme application de courrier électronique par défaut.
Cliquez sur « Installer » pour continuer.
< Précédent
Installer
Annuler

Figure 2: La fenêtre Mozilla Thunderbird - Résumé

Quatrième étape. **Cliquez** sur Installer pour lancer le processus d'installation. La barre de progression **Mozilla Thunderbird - Installation** s'affiche alors. Lorsque le processus d'installation est terminé, la fenêtre suivante s'affiche:

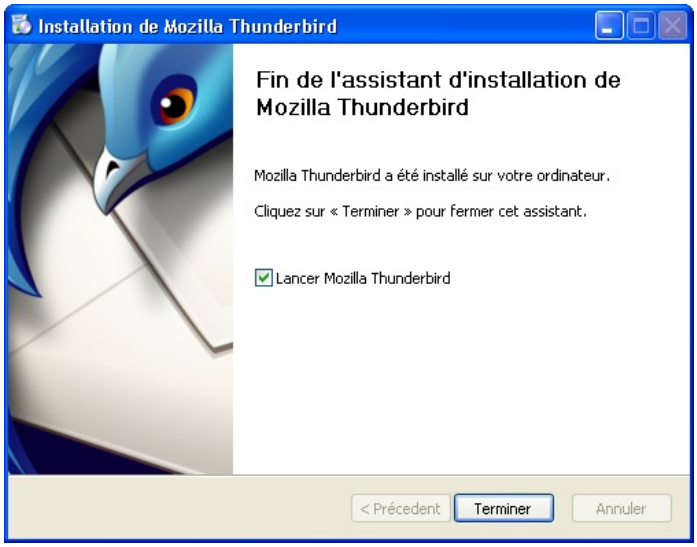

Installation de Mozilla Thunderbird
Fin de l'assistant d'installation de Mozilla Thunderbird
Mozilla Thunderbird a été installé sur votre ordinateur.
Cliquez sur « Terminer » pour fermer cet assistant.
Lancer Mozilla Thunderbird
< Précédent
Terminer
Annuler

Figure 3: La fenêtre Fin de l'assistant d'installation de Mozilla Thunderbird

Cinquième étape. **Cliquez** sur Terminer pour compléter le processus d'installation.

Astuce: **Thunderbird** se lancera automatiquement si l'option *Lancer Mozilla Thunderbird* est cochée, tel qu'illustré à la *figure 3* ci-dessus. Pour lancer le programme à l'avenir, vous pouvez, soit **double-cliquer** sur l'icone de bureau de **Thunderbird**, soit **sélectionner > Programmes > Mozilla Thunderbird > Mozilla Thunderbird**.

2.1 Comment désactiver l'option Recherche et indexation globales dans Thunderbird

Attention: La fonction *Recherche et indexation globales* de **Thunderbird** *doit* être désactivée pour optimiser la performance du programme. Selon la quantité et la taille de vos messages, cette fonction peut ralentir votre système et réécrivant continuellement et inutilement les mêmes données sur votre disque dur. Au fur et à mesure que votre disque dur se remplit, plusieurs opérations de votre système tourneront de plus en plus au ralentit.

Pour désactiver l'option *Recherche et indexation globales*, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Outils > Options** dans la console **Thunderbird** pour afficher la fenêtre *Options*.

Deuxième étape. **Cliquez** sur Avancé pour afficher le contenu de cet onglet:

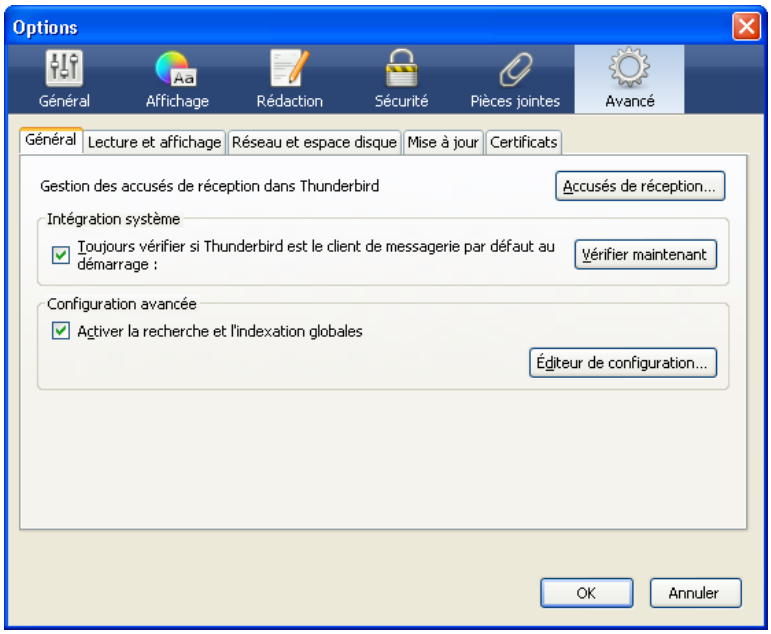


Figure 4: La fenêtre Options affichant le contenu de l'onglet Avancé

Troisième étape. **Cliquez** sur la case *Activer la recherche et l'indexation globales*, dans la section *Configuration avancée*, pour *désactiver* cette option, tel qu'illustré ci-dessous:

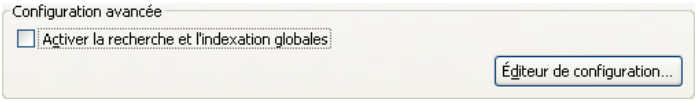


Figure 5: La section Configuration avancée

Maintenant que vous avez désactivé cette option, vous êtes prêt à enregistrer un compte de courrier électronique dans **Thunderbird**.

2.2 Comment enregistrer un compte de courrier électronique dans Thunderbird

La fenêtre *Assistant d'importation - Importer les paramètres et les dossiers de messages* n'apparaît qu'à la première installation de **Thunderbird**.

Première étape. **Cochez** l'option *Ne rien importer*, tel qu'illustré ci-dessous:

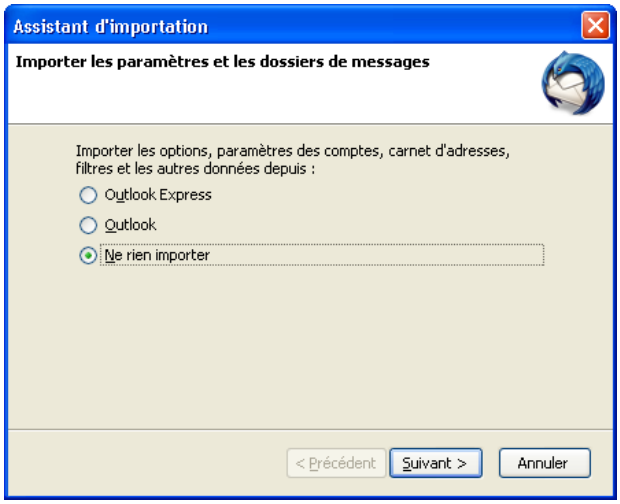
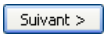

Assistant d'importation
Importer les paramètres et les dossiers de messages
Importer les options, paramètres des comptes, carnet d'adresses, filtres et les autres données depuis :
Outlook Express
Outlook
Ne rien importer
< Précédent
Suivant >
Annuler

Figure 6: L'Assistant d'importation - Importer les paramètres et les dossiers de messages

Deuxième étape. **Cliquez** sur  pour afficher la fenêtre suivante:

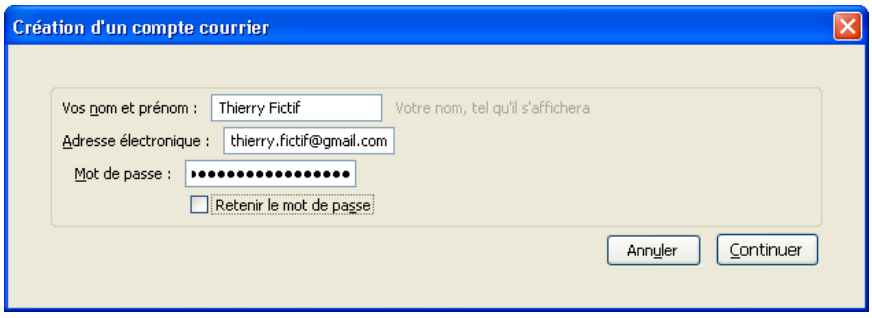

Création d'un compte courrier
Vos nom et prénom : Thierry Fictif
Votre nom, tel qu'il s'affichera
Adresse électronique : thierry.fictif@gmail.com
Mot de passe : ••••••••••••••••
Retenir le mot de passe
Annuler
Continuer

Figure 7: La fenêtre Création d'un compte courrier

Troisième étape. **Saisissez** votre nom, adresse de courrier électronique et mot de passe dans les champs appropriés; puis **décochez** l'option *Retenir le mot de passe*, tel qu'illustré à la *figure 7* ci-dessous.

Quatrième étape. **Cliquez** sur Continuer pour afficher la fenêtre suivante:

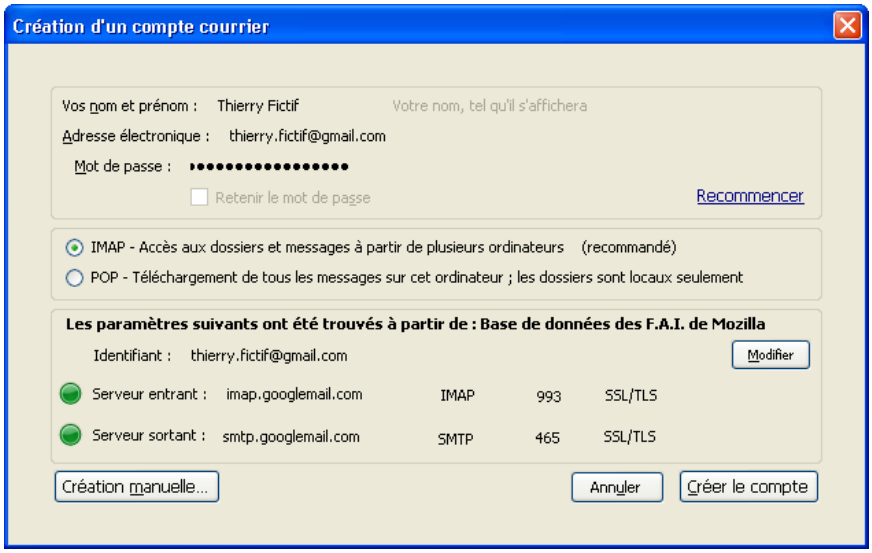

Création d'un compte courrier
Vos nom et prénom : Thierry Fictif
Votre nom, tel qu'il s'affichera
Adresse électronique : thierry.fictif@gmail.com
Mot de passe : ••••••••••••••••
Retenir le mot de passe
Recommencer
IMAP - Accès aux dossiers et messages à partir de plusieurs ordinateurs (recommandé)
POP - Téléchargement de tous les messages sur cet ordinateur ; les dossiers sont locaux seulement
Les paramètres suivants ont été trouvés à partir de : Base de données des F.A.I. de Mozilla
Identifiant : thierry.fictif@gmail.com
Modifier
Serveur entrant : imap.googlemail.com IMAP 993 SSL/TLS
Serveur sortant : smtp.googlemail.com SMTP 465 SSL/TLS
Création manuelle...
Annuler
Créer le compte

*Figure 8: La fenêtre Création d'un compte courrier avec l'option **IMAP - Accès aux dossiers et messages à partir de plusieurs ordinateurs** sélectionnée*

IMAP et POP: Descriptions et utilisation

Internet Message Access Protocol (**IMAP**) et **Post Office Protocol** (**POP**) sont deux méthodes distinctes d'archiver et de recevoir des messages de courrier électronique.

- **Internet Message Access Protocol** (**IMAP**): Lorsque vous utilisez la méthode **IMAP**, tous vos dossiers (y compris les dossiers *Courrier entrant*, *Brouillons*, *Envoyés*, *Corbeille* et tous les autres dossiers) demeure sur le serveur de courrier. De cette façon, vous pouvez accéder à ces dossiers depuis un autre ordinateur. Tous les messages seront donc conservés sur le serveur et, initialement, seulement le titre des messages (comportant des renseignements comme la date et l'heure, le sujet du message, le nom de l'expéditeur, etc.) sont téléchargés pour être affichés par votre client mail sur votre ordinateur. Les messages complets ne sont affichés que lorsque vous cliquez dessus pour les ouvrir. **Thunderbird** peut aussi être configuré pour archiver dans votre ordinateur des copies de vos messages qui se trouvent dans certains ou dans tous vos dossiers, afin que vous puissiez travailler dessus en mode autonome (non connecté à Internet). En mode **IMAP**, lorsque vous supprimé des messages ou des dossiers, vous le faites *à la fois* sur votre ordinateur local et sur le serveur.

- **Post Office Protocol** (**POP**): Lorsque vous utilisez la méthode **POP**, seul le dossier *Courrier entrant* (le dossier où sont livrés et affichés les nouveaux messages entrants) demeure sur le serveur distant; tous les autres dossiers sont situés sur votre ordinateur local seulement. Vous pouvez choisir de laisser vos messages dans le dossier *Courrier entrant* sur le serveur après les avoir téléchargés sur votre ordinateur, ou vous pouvez les supprimer du serveur. Dans le dernier cas, si vous accédez à votre compte depuis un autre ordinateur, vous ne verrez uniquement que les messages du dossier *Courrier entrant* (les nouveaux messages et ceux que vous avez choisi de ne pas supprimé du serveur).

Cinquième étape. **Cliquez** sur Créer le compte pour créer votre compte et afficher la console **Thunderbird** avec votre compte de courrier compris dans la barre *Tous les dossiers*, à gauche, tel qu'illustré ci-dessous:

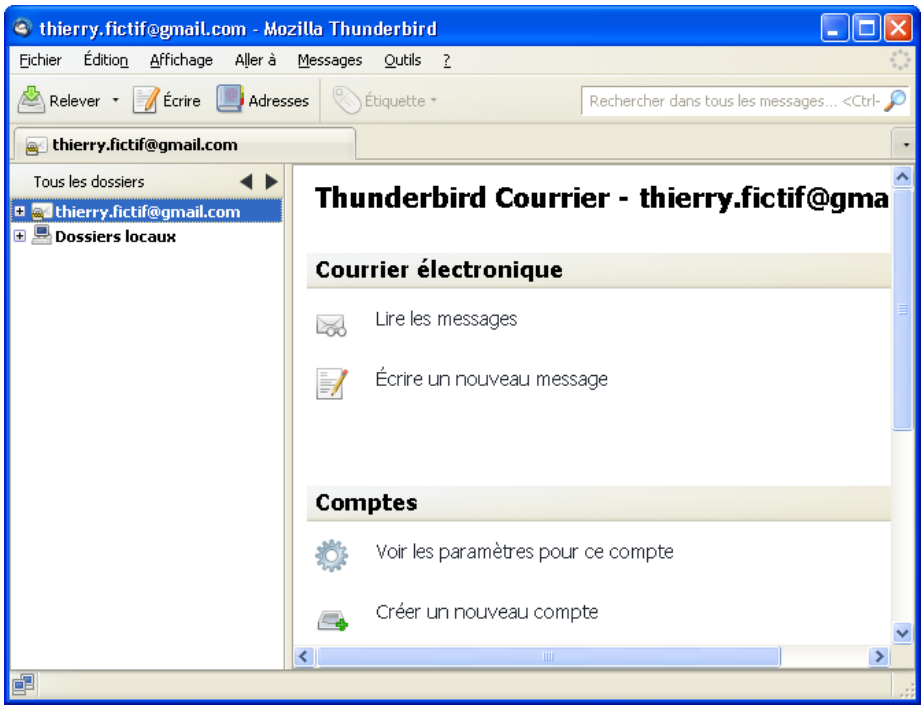


Figure 9: L'interface principale de Thunderbird affichant votre compte Gmail nouvellement enregistré

Commentaire: Pour ajouter un autre compte de courriel, **sélectionnez Fichier > Nouveau > Comptes courrier...** pour afficher la *figure 7* de cette section, et reprenez les **étapes 3 à 5**.

Après avoir enregistré vos comptes de courrier électronique dans **Thunderbird**, la prochaine fois que vous ouvrirez l'interface principale, on vous demandera de saisir votre mot de passe pour chaque compte, comme suit:

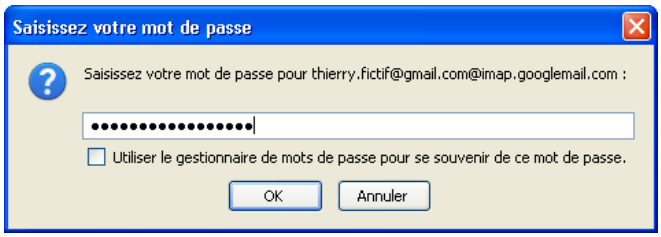

Saisissez votre mot de passe
Saisissez votre mot de passe pour thierry.fictif@gmail.com@imap.googlemail.com :
Utiliser le gestionnaire de mots de passe pour se souvenir de ce mot de passe.
OK
Annuler

Figure 10: La fenêtre Saisissez votre mot de passe

Commentaire: Bien que la fonction d'enregistrement du mot de passe ne soit généralement pas recommandée, **Thunderbird** comporte une fonction de *Mot de passe maître*. Cette fonction permet de n'utiliser qu'un seul mot de passe pour protéger tous les mots de passes associés à vos différents comptes, que vous ne saisissez qu'une seule fois lors du processus d'enregistrement. Pour plus de renseignements sur cette fonction, veuillez consulter la section **3.3 Comment configurer les onglets de sécurité dans Thunderbird** [152] **- L'onglet Mot de passe**.

2.3 Comment enregistrer des comptes de blogs, de nouvelles et de groupes de discussion

Pour créer et enregistrer un compte pour des blogs, des nouvelles ou des groupes de discussion, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez > Fichier > Nouveau > Autres comptes** pour afficher la fenêtre *Assistant de création de compte > Paramétrage du nouveau compte*.

Deuxième étape. **Cochez** soit l'option *Blogs et nouvelles*, soit l'option *Groupes de discussion*, puis **cliquez** sur Suivant > pour afficher la fenêtre suivante:

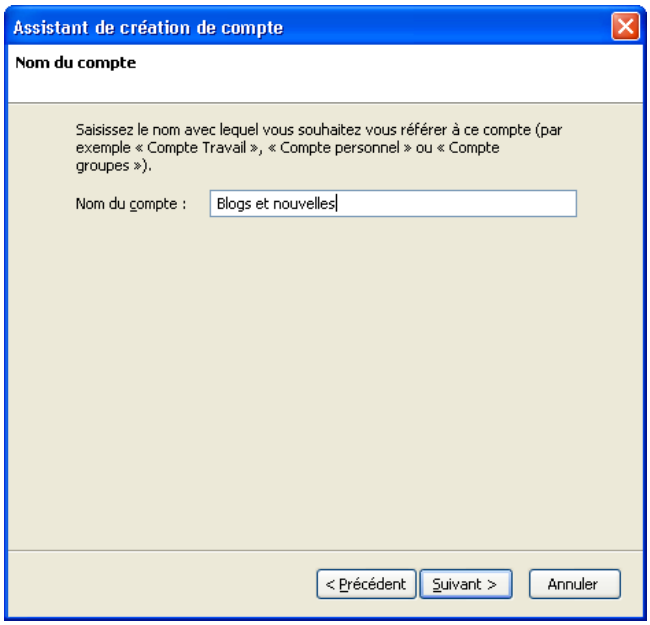

Assistant de création de compte
Nom du compte
Saisissez le nom avec lequel vous souhaitez vous référer à ce compte (par exemple « Compte Travail », « Compte personnel » ou « Compte groupes »).
Nom du compte :
Blogs et nouvelles
< Précédent
Suivant >
Annuler

Figure 11: La fenêtre Assistant de création de compte - Nom du compte

Troisième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

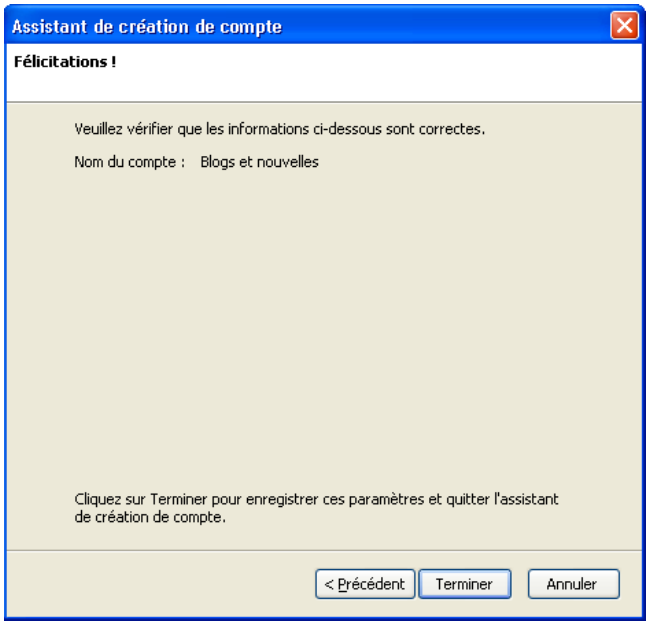

Assistant de création de compte
Félicitations !
Veuillez vérifier que les informations ci-dessous sont correctes.
Nom du compte : Blogs et nouvelles
Cliquez sur Terminer pour enregistrer ces paramètres et quitter l'assistant de création de compte.
< Précédent
Terminer
Annuler

Figure 12: La fenêtre Assistant de création de compte - Félicitations!

Cinquième étape. **Cliquez** sur Terminer pour compléter le processus d'enregistrement du compte et retourner à la console **Thunderbird**.

Maintenant que vous avez configuré **Thunderbird** pour une utilisation optimale, veuillez lire la prochaine section, **Comment régler les options de sécurité dans Thunderbird** [153].

Comment régler les options de sécurité dans Thunderbird

Sommaire des sections de cette page:

- **3.0 À propos des options de sécurité de Thunderbird**
- **3.1 Comment désactiver le panneau d'affichage des messages de Thunderbird**
- **3.2 Comment désactiver la fonction HTML dans Thunderbird**
- **3.3 Comment régler les options de sécurité dans Thunderbird**
- **3.4 Comment activer le filtre des indésirables dans les paramètres du compte**

3.0 À propos des options de sécurité de Thunderbird

Dans le contexte de **Mozilla Thunderbird**, le terme 'sécurité' fait référence à la protection de votre ordinateur contre des messages de courrier électronique nuisibles ou malveillants. Il peut s'agir de pourriel, par exemple, ou encore de messages servant de véhicules à des virus ou des logiciels espions. Il existe plusieurs paramètres qui doivent être activés, désactivés ou

réglés adéquatement dans **Mozilla Thunderbird** pour permettre au programme de défendre efficacement votre système contre des attaques provenant du courrier électronique. Il est également *absolument impératif* que vous installiez des logiciels pare-feu, antivirus et anti-mouchards.

Pour plus de renseignements sur les moyens de prévenir les intrusions nuisibles ou malveillantes, veuillez consulter le chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** [4] du **Livret pratique**, ainsi que les chapitres portant sur **Avast** [154], **Comodo Firewall** [155] et **Spybot** [156].

3.1 Comment désactiver le panneau d'affichage des messages de Thunderbird

La console **Thunderbird** est séparée en trois sections distinctes: l'encadré à gauche affiche les différents dossiers de vos comptes de courriel; le panneau à droite affiche une liste de messages; et le panneau du bas à droite affiche un *aperçu* d'un message sélectionné.

Commentaire: Si un message contient du code malicieux, ce panneau affichant l'aperçu du message pourrait l'activer; il est donc recommandé de le désactiver.

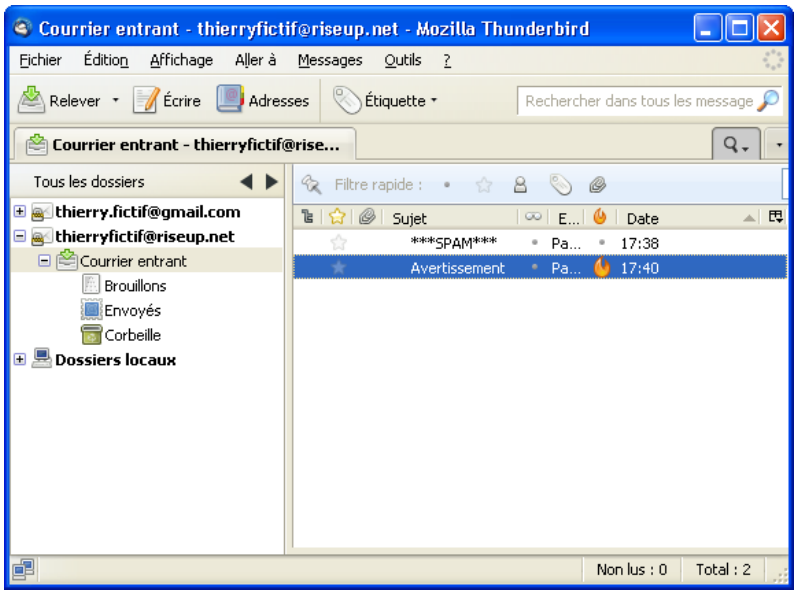


Figure 1: L'interface principale de Thunderbird

Pour désactiver le panneau d'affichage des messages, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Affichage > Disposition**, puis **dessélectionnez** l'option *Panneau d'affichage des messages* pour la désactiver, comme suit:

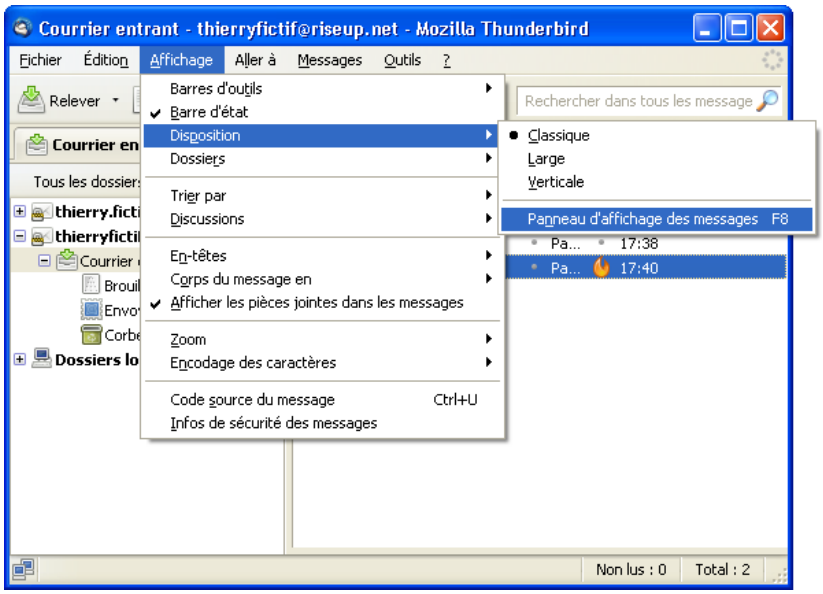


Figure 2: Le menu Affichage affichant le sous-menu Disposition avec le Panneau d'affichage des messages sélectionné

Le *Panneau d'affichage des messages* n'apparaitra plus et vous devrez désormais **double-cliquer** sur un message pour en afficher le contenu. Si un message vous semble suspect (parce que son titre, par exemple, est impertinent ou inattendu, ou parce qu'il provient d'un expéditeur inconnu), vous pouvez maintenant le supprimer avant d'en afficher le contenu.

3.2 Comment désactiver la fonction HTML dans Thunderbird

Thunderbird vous permet d'utiliser le **HyperText Markup Language** (**HTML**) pour composer vos messages. Cela signifie que

vous pouvez recevoir ou envoyer des messages qui comprennent des couleurs, des polices spéciales, des images et d'autres options de mise en page. Par contre, le **HTML** est le même langage utilisé pour coder des pages Web; l'affichage de messages codés en **HTML** peut vous exposer à des codes malveillants, ce qui comporte certains des mêmes risques que ceux posés par les sites Internet.

Pour désactiver la fonction de mise en page **HTML**, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Affichage > Corps du message en > Texte seul**, comme suit:

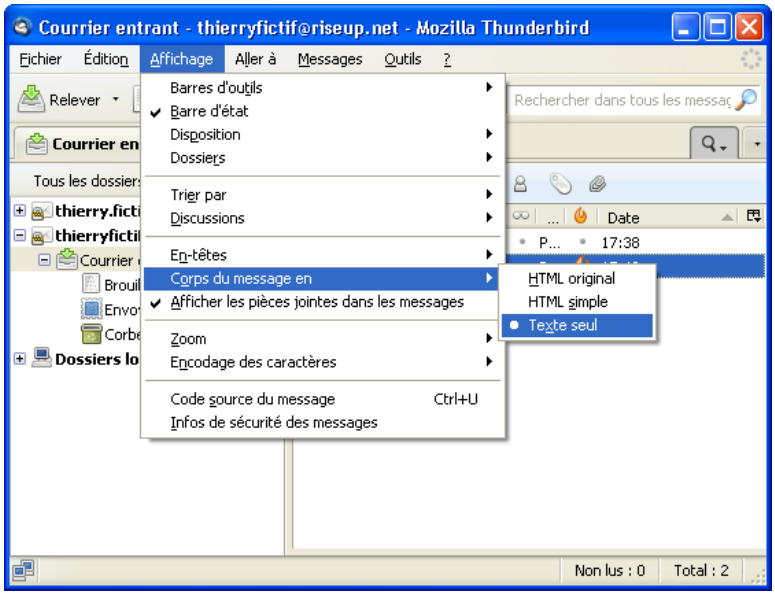


Figure 3: Le menu Affichage affichant le sous-menu Corps du message en avec l'option Texte seul sélectionné

3.3 Comment régler les options de sécurité

Thunderbird comporte deux filtres de courrier indésirable qui peuvent vous aider à déterminer quels messages sont des pourriels. Par défaut, ces filtres sont désactivés et vous devez donc les activer avant de les utiliser. Même après les avoir désactivés, vous continuerez à recevoir du courrier indésirable, mais **Thunderbird** les classera automatiquement dans le dossier *Indésirables*.

Le courrier frauduleux, aussi appelés messages d'*hammeçonnage*, ou *phishing*, essaie habituellement de vous faire cliquer sur des liens qui sont codés dans le message. Souvent, ces liens redirigent votre navigateur vers des sites Internet qui tenteront d'infecter votre ordinateur avec un virus. Dans d'autres cas, le lien vous mènera vers un site Internet qui semble légitime, mais qui est en fait conçu pour vous induire à révéler vos noms d'utilisateurs et vos mots de passe, qui pourront ensuite être utilisés ou vendus à une tierce partie à des fins commerciales ou malveillantes.

Thunderbird peut identifier ce type de courrier et vous en avertir. Des outils supplémentaires peuvent prévenir les infections provenant de sites Internet malveillants: voir la section **Autres modules utiles de Mozilla** [157] du chapitre portant sur **Firefox**.

Le premier ensemble de paramètres de sécurité concernant le courrier indésirable se trouve dans la fenêtre *Options - Sécurité*, où la majorité des options de sécurité et de confidentialité peuvent être réglées. Pour y accéder, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Outils > Options** pour afficher la fenêtre *Options*.

Deuxième étape. **Cliquez** sur

pour afficher la fenêtre suivante:

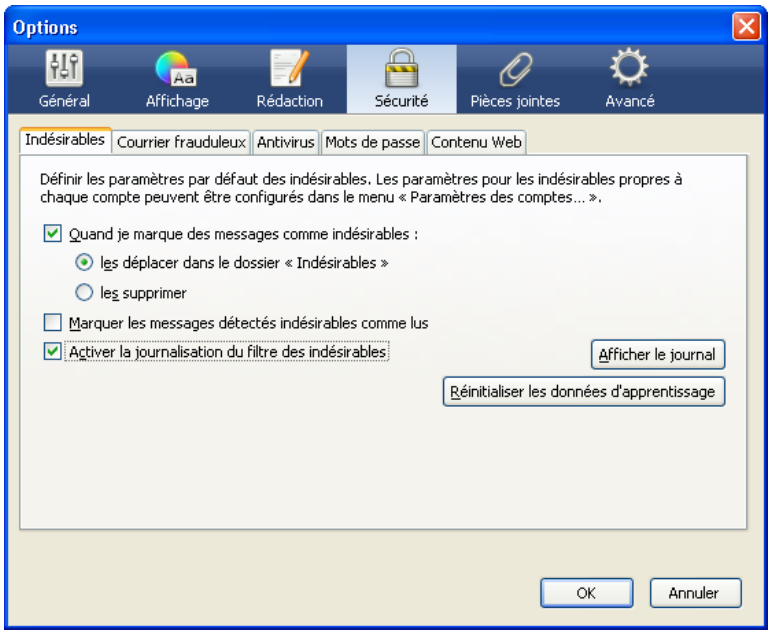


Figure 4: La fenêtre Sécurité affichant le contenu de l'onglet Indésirables

L'onglet Indésirables

Première étape. **Cochez** les options pertinentes dans l'onglet *Indésirables*, tel qu'illustré à la *figure 4*, ci-dessus, pour permettre à **Thunderbird** de supprimer les messages que vous définis comme courrier indésirable. D'autres options de filtrage du courrier indésirable seront abordés plus loin dans cette section.

L'onglet Courrier frauduleux

Première étape. **Cochez** l'option *Signaler si le message en cours de lecture est susceptible d'être frauduleux* pour permettre à **Thunderbird** d'analyser les messages pour y détecter des fraudes potentielles:

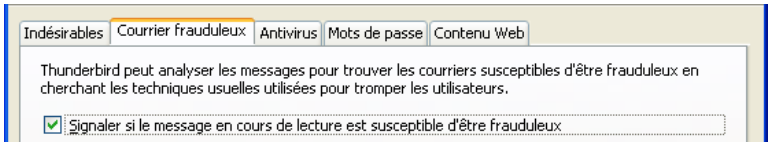

Indésirables
Courrier frauduleux
Antivirus
Mots de passe
Contenu Web
Thunderbird peut analyser les messages pour trouver les courriers susceptibles d'être frauduleux en cherchant les techniques usuelles utilisées pour tromper les utilisateurs.
Signaler si le message en cours de lecture est susceptible d'être frauduleux

Figure 5: L'onglet Courrier frauduleux

L'onglet Antivirus

Première étape. **Cliquez** sur l'onglet *Antivirus* pour afficher la fenêtre suivante:

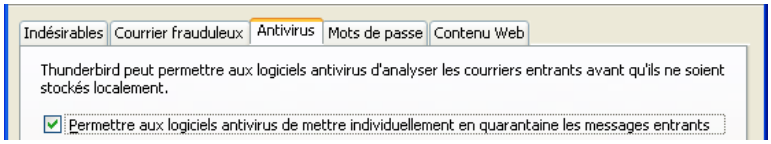

Indésirables
Courrier frauduleux
Antivirus
Mots de passe
Contenu Web
Thunderbird peut permettre aux logiciels antivirus d'analyser les courriers entrants avant qu'ils ne soient stockés localement.
Permettre aux logiciels antivirus de mettre individuellement en quarantaine les messages entrants

Figure 6: L'onglet Antivirus

Cette option permet à votre logiciel antivirus de scanner et d'isoler des messages individuellement au fur et à mesure qu'ils arrivent. Si cette option n'est pas activée, il est possible que votre dossier *Courrier entrant au complet* soit placé 'en quarantaine' si vous recevez ne serait-ce qu'un seul message infecté.

Commentaire: Il est tenu pour acquis qu'il y a un programme antivirus fonctionnel installé sur votre ordinateur. Veuillez consulter le chapitre portant sur **Avast** [27] pour plus de renseignements sur l'installation et la configuration d'un logiciel antivirus.

L'onglet Mots de passe

Première étape. **Cliquez** sur l'onglet *Mots de passe* pour afficher la fenêtre suivante:

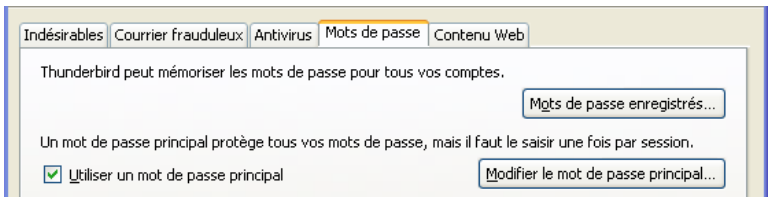

Indésirables
Courrier frauduleux
Antivirus
Mots de passe
Contenu Web
Thunderbird peut mémoriser les mots de passe pour tous vos comptes.
Mots de passe enregistrés...
Un mot de passe principal protège tous vos mots de passe, mais il faut le saisir une fois par session.
Utiliser un mot de passe principal
Modifier le mot de passe principal...

Figure 7: L'onglet Mots de passe

Important: Nous recommandons fortement que vous gardiez vos mots de passe privés en utilisant un programme conçu spécialement à cette fin; veuillez consulter le chapitre portant sur **KeyPass** [77] pour plus de renseignements à ce sujet.

Commentaire: Les options de l'onglet *Mots de passe* ne fonctionneront que si vous sélectionnez d'abord l'option *Retenir le mot de passe* dans la toute première fenêtre d'enregistrement d'un compte courrier dans **Thunderbird**.

Deuxième étape. **Cliquez** sur Mots de passe enregistrés... pour afficher la fenêtre suivante:

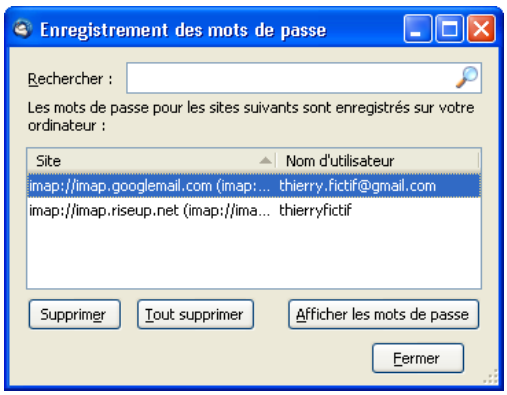


Figure 8: La fenêtre Enregistrement des mots de passe

La fenêtre *Enregistrement des mots de passe* vous permet de supprimer ou d'afficher les mots de passe correspondant à chacun de vos comptes. Cela dit, pour maximiser votre sécurité et la confidentialité de vos renseignements, vous pouvez également définir un *Mot de passe principal* pour faire en sorte que vos mots de passe ne soit pas accessibles aux personnes qui sont le moindrement familière avec les options de mots de passe de **Thunderbird**.

Troisième étape. **Cochez** l'option *Utiliser un mot de passe principal*, tel qu'illustré à la *figure 7* pour activer le bouton *Modifier le mot de passe principal*.

Quatrième étape. **Cliquez** sur Modifier le mot de passe principal... pour afficher la fenêtre suivante:

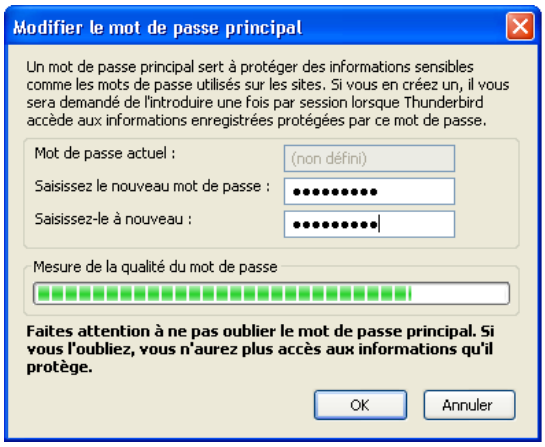

Modifier le mot de passe principal
Un mot de passe principal sert à protéger des informations sensibles comme les mots de passe utilisés sur les sites. Si vous en créez un, il vous sera demandé de l'introduire une fois par session lorsque Thunderbird accède aux informations enregistrées protégées par ce mot de passe.
Mot de passe actuel :
(non défini)
Saisissez le nouveau mot de passe :
Saisissez-le à nouveau :
Mesure de la qualité du mot de passe
Faites attention à ne pas oublier le mot de passe principal. Si vous l'oubliez, vous n'aurez plus accès aux informations qu'il protège.
OK
Annuler

Figure 9: La fenêtre Modifier le mot de passe principal

Cinquième étape. **Saisissez** un mot de passe suffisamment difficile, que vous seul connaîtrez, puis **cliquez** sur OK pour confirmer votre *Mot de passe principal*. La prochaine fois que vous **cliquerez** sur Mots de passe enregistrés..., la fenêtre suivante apparaîtra pour vous demander de saisir votre mot de passe principal:

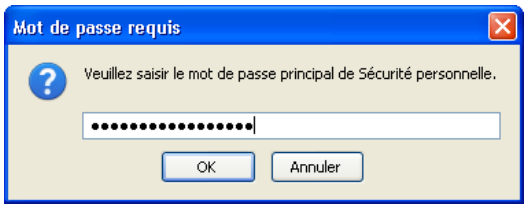


Figure 10: La fenêtre Mot de passe requis

L'onglet Contenu Web

Un cookie est un minuscule texte codé que votre navigateur web utilise pour authentifier ou identifier un site Internet donné. L'onglet *Contenu Web* vous permet de spécifier quels cookies de blogs, de nouvelles ou de groupes de discussions sont sûrs et fiables.

Première étape. **Cliquez** sur l'onglet *Contenu Web* pour afficher la fenêtre suivante:

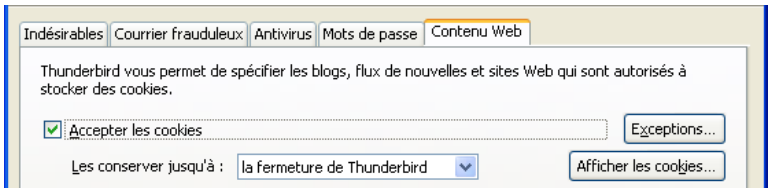

Indésirables
Courrier frauduleux
Antivirus
Mots de passe
Contenu Web
Thunderbird vous permet de spécifier les blogs, flux de nouvelles et sites Web qui sont autorisés à stocker des cookies.
Accepter les cookies
Exceptions...
Les conserver jusqu'à :
la fermeture de Thunderbird
Afficher les cookies...

Figure 11: L'onglet Contenu Web

Deuxième étape. **Sélectionnez** l'option *la fermeture de Thunderbird* dans la liste *Les conserver jusqu'à:* pour supprimer les cookies lorsque vous fermez **Thunderbird**, pour une plus grande sécurité.

3.4 Comment activer le filtre des indésirables dans les paramètres du compte

Le deuxième type de filtrage du courrier indésirable offert par **Thunderbird** se trouve dans la fenêtre *Paramètres des comptes - Paramètres pour les indésirables*. Par défaut, ces filtres sont désactivés et vous devrez donc les activer pour les utiliser. Lorsque des messages indésirables arrivent, **Thunderbird** les classera automatiquement dans les dossiers *Indésirables* associés à chaque compte.

Première étape. **Sélectionnez Outils > Paramètres des comptes** pour afficher la fenêtre *Paramètres des comptes*.

Deuxième étape. **Sélectionnez** l'option *Paramètres des indésirables* associé à un compte **Gmail** ou **RiseUp** dans l'encadré de gauche.

Troisième étape. **Réglez** les options des *Paramètres des indésirables* de sorte que vos *Paramètres de comptes - Paramètres des indésirables* ressemblent à ceci:

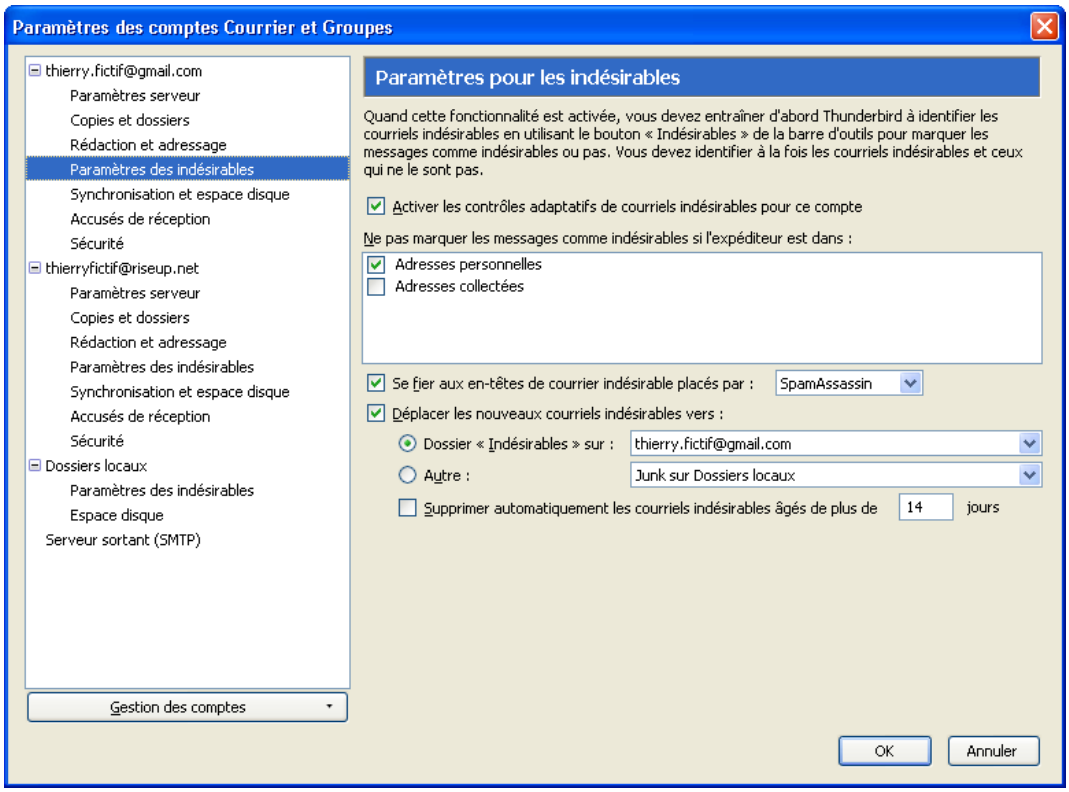

Paramètres des comptes Courrier et Groupes
thierry.fictif@gmail.com
Paramètres serveur
Copies et dossiers
Rédaction et adressage
Paramètres des indésirables
Synchronisation et espace disque
Accusés de réception
Sécurité
thierryfictif@riseup.net
Paramètres serveur
Copies et dossiers
Rédaction et adressage
Paramètres des indésirables
Synchronisation et espace disque
Accusés de réception
Sécurité
Dossiers locaux
Paramètres des indésirables
Espace disque
Serveur sortant (SMTP)
Gestion des comptes
Paramètres pour les indésirables
Quand cette fonctionnalité est activée, vous devez entraîner d'abord Thunderbird à identifier les courriels indésirables en utilisant le bouton « Indésirables » de la barre d'outils pour marquer les messages comme indésirables ou pas. Vous devez identifier à la fois les courriels indésirables et ceux qui ne le sont pas.
Activer les contrôles adaptatifs de courriels indésirables pour ce compte
Ne pas marquer les messages comme indésirables si l'expéditeur est dans :
Adresses personnelles
Adresses collectées
Se fier aux en-têtes de courrier indésirable placés par :
SpamAssassin
Déplacer les nouveaux courriels indésirables vers :
Dossier « Indésirables » sur :
thierry.fictif@gmail.com
Autre :
Junk sur Dossiers locaux
Supprimer automatiquement les courriels indésirables âgés de plus de
14
jours
OK
Annuler

Figure 12: La fenêtre Paramètres des comptes - Paramètres des indésirables

Quatrième étape. **Cliquez** sur OK pour compléter la configuration de la fenêtre *Paramètres des comptes*.

Commentaire: Les options des *Paramètres des indésirables* doivent être réglés séparément pour chaque compte. Ainsi, les indésirables des compte *Gmail* ou *Riseup* seront placés dans leur dossier *Supprimés* respectif. Sinon, vous pouvez également désigner un *Dossier local* pour recevoir les indésirables de tous vos comptes.

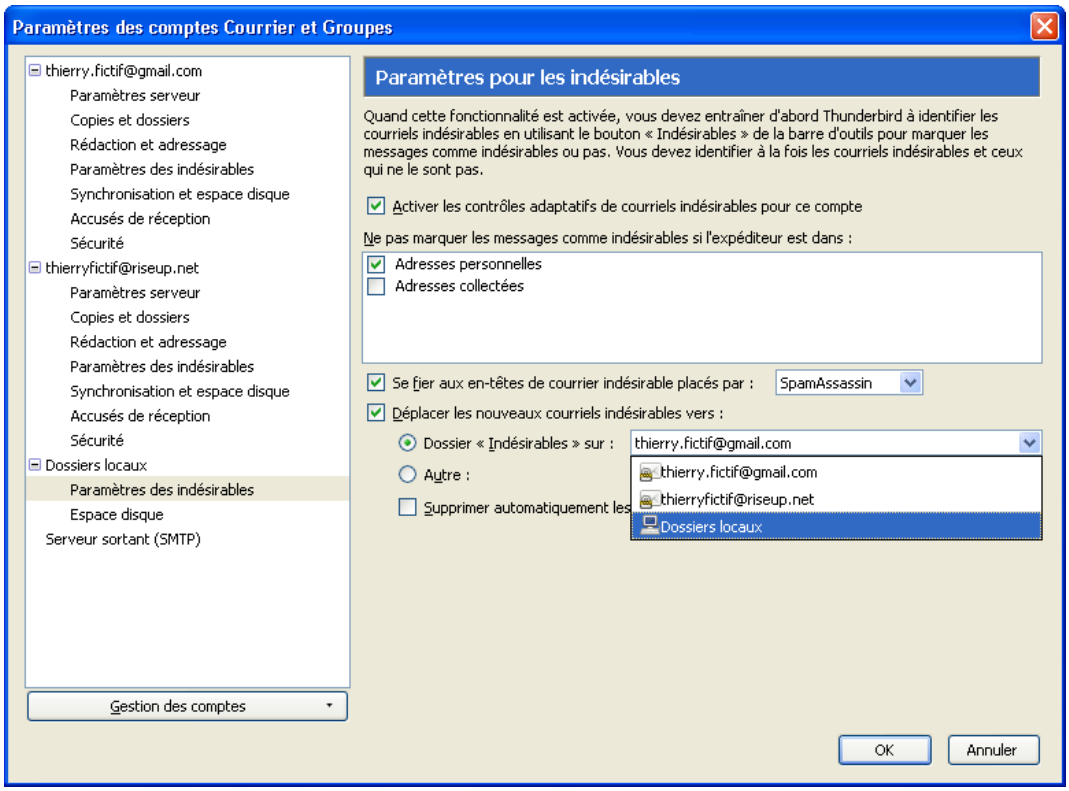

Paramètres des comptes Courrier et Groupes
thierry.fictif@gmail.com
Paramètres serveur
Copies et dossiers
Rédaction et adressage
Paramètres des indésirables
Synchronisation et espace disque
Accusés de réception
Sécurité
thierryfictif@riseup.net
Paramètres serveur
Copies et dossiers
Rédaction et adressage
Paramètres des indésirables
Synchronisation et espace disque
Accusés de réception
Sécurité
Dossiers locaux
Paramètres des indésirables
Espace disque
Serveur sortant (SMTP)
Gestion des comptes
Paramètres pour les indésirables
Quand cette fonctionnalité est activée, vous devez entraîner d'abord Thunderbird à identifier les courriels indésirables en utilisant le bouton « Indésirables » de la barre d'outils pour marquer les messages comme indésirables ou pas. Vous devez identifier à la fois les courriels indésirables et ceux qui ne le sont pas.
Activer les contrôles adaptatifs de courriels indésirables pour ce compte
Ne pas marquer les messages comme indésirables si l'expéditeur est dans :
Adresses personnelles
Adresses collectées
Se fier aux en-têtes de courrier indésirable placés par :
SpamAssassin
Déplacer les nouveaux courriels indésirables vers :
Dossier « Indésirables » sur :
thierry.fictif@gmail.com
Autre :
Supprimer automatiquement les
thierry.fictif@gmail.com
thierryfictif@riseup.net
Dossiers locaux
OK
Annuler

Figure 13: La fenêtre Paramètres des comptes - Paramètres des indésirables affichant les réglages pour un dossier Indésirables central

Première étape. **Sélectionnez** l'option *Paramètres des indésirables* sous la rubrique *Dossiers locaux* dans l'encadré de gauche.

Deuxième étape. **Sélectionnez** l'option *Dossiers locaux* dans la liste défilante *Dossier Indésirables sur:*, tel qu'illustré à la *figure 13*.

Troisième étape. **Cliquez** sur OK pour compléter la configuration de la fenêtre *Paramètres des comptes*.

Maintenant que vous avez configuré les diverses options de sécurité et de gestion des indésirables de **Thunderbird**, veuillez lire la prochaine section, **Comment utiliser Enigmail avec GnuPG dans Thunderbird** [158].

Comment utiliser Enigmail avec GnuPG dans Thunderbird

Sommaire de sections de cette page:

- **4.0 Un aperçu d'Enigmail, de GnuPG et du chiffrement asymétrique (à clé privée)**
- **4.1 Comment installer Enigmail et GnuPG**
- **4.2 Comment générer des paires de clés et configurer Enigmail pour qu'il fonctionne avec vos comptes de courriel**
- **4.3 Comment échanger des clés publiques**
- **4.4 Comment valider et signer un paire de clés**
- **4.5 Comment chiffrer et déchiffrer des messages**

4.0 Un aperçu d'Enigmail, de GnuPG et du chiffrement asymétrique (à clé privée)

Enigmail est un module complémentaire de **Mozilla Thunderbird** qui vous permet de protéger la confidentialité de vos communications par courrier électronique. **Enigmail** n'est rien d'autre qu'une interface graphique conçue pour faciliter l'utilisation du programme de chiffrement **GnuPG** avec **Thunderbird**. L'interface d'**Enigmail** est représentée par un lien *OpenPGP* dans la barre d'outils de la console **Thunderbird**.

Enigmail emploie la méthode de **cryptographie asymétrique, ou cryptographie à clé publique** [159]. En vertu de cette méthode, chaque individu doit générer sa propre paire de clés. La première clé est dite *privée*. Celle-ci est protégée par un mot de passe complexe, gardée secrète et *jamais* partagée avec *qui que ce soit*.

La deuxième clé est dite *publique*. Cette clé peut être partagée avec vos correspondants. Lorsque vous avez la *clé publique* d'un correspondant, vous pouvez commencer à envoyer des messages chiffrés à cette personne. Elle, et elle seule, sera en mesure de déchiffrer et de lire vos messages, car elle est la seule personne qui dispose de la *clé privée* correspondante.

De la même façon, si vous envoyez une copie de votre propre *clé publique* à tous vos contacts et gardez la *clé privée* secrète, vous et vous seul serez en mesure de lire les messages chiffrés que vous enverront vos contacts.

Enigmail vous permet également d'attacher des *signatures numériques* à vos messages. Le destinataire de votre message qui dispose d'une copie légitime de votre clé publique pourra vérifier que le message provient bel et bien de vous, et que son

contenu n'a pas été altéré en chemin. En échange, si vous avez la clé publique d'un correspondant, vous pouvez vérifier la signature numérique de ses messages.

4.1 Comment installer Enigmail et GnuPG

Veuillez consulter la section **Téléchargement** [117] pour obtenir les consignes de téléchargement d'**Enigmail** et de **GnuPG**.

4.1.1 Comment installer GnuPG

L'installation de **GnuPG** est très simple et ressemble au processus d'installation de programmes que vous avez déjà probablement déjà effectué.

Pour installer **GnuPG**, suivez les étapes énumérées ci-dessous:

Première étape. **Double-cliquez** sur gnupg-w32cli-1.4.11 pour lancer le processus d'installation. Il est possible que la boîte di dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche. Si c'est le cas, **cliquez** sur Exécuter pour afficher la fenêtre suivante:

GNU Privacy Guard Setup
Welcome to the GNU Privacy Guard Setup Wizard
GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC4880.
Click Next to continue.
This is GnuPG version 1.4.11
built on 2010-10-18 10:04 UTC
file version 1.4.11.29110
Next >
Cancel

Figure 1: L'assistant d'installation de GNU Privacy Guard

Deuxième étape. **Cliquez** sur Next > pour afficher la fenêtre *GNU Privacy Guard Setup - License Agreement*; après l'avoir lu, **cliquez** sur Next > pour afficher la fenêtre *GNU Privacy Guard Setup - Choose Components*.

Troisième étape. **Cliquez** sur Next > pour accepter les paramètres par défaut et afficher la fenêtre *GNU Privacy Guard Setup - Install Options - GnuPG Language Selection*.

Quatrième étape. **Sélectionnez** *fr-Français* dans la liste défilante, puis **Cliquez** sur Next > pour afficher la fenêtre *Choose Install Location*.

Cinquième étape. **Cliquez** sur Next > pour accepter l'emplacement par défaut et afficher la fenêtre *Choose Start Menu Folder*.

Sixième étape. **Cliquez** sur Install pour installer **GnuPG**. Lorsque ce processus est complété, la fenêtre *Installation Complete* s'affiche.

Septième étape. **Cliquez** sur Next >, puis sur Finish pour finaliser l'installation du programme **GnuPG**.

4.1.2 Comment installer le module complémentaire Enigmail

Après avoir complété l'installation du programme **GnuPG**, il vous faut installer le module complémentaire **Enigmail**.

Pour lancer l'installation d'**Enigmail**, suivez les étapes énumérées ci-dessous:

Première étape. **Ouvrez Thunderbird**, puis **sélectionnez Outils > Modules complémentaires** pour afficher la fenêtre *Modules complémentaires*; le panneau *Catalogue* sera affiché par défaut.

Deuxième étape. **Cliquez** sur Extensions pour afficher la fenêtre suivante:

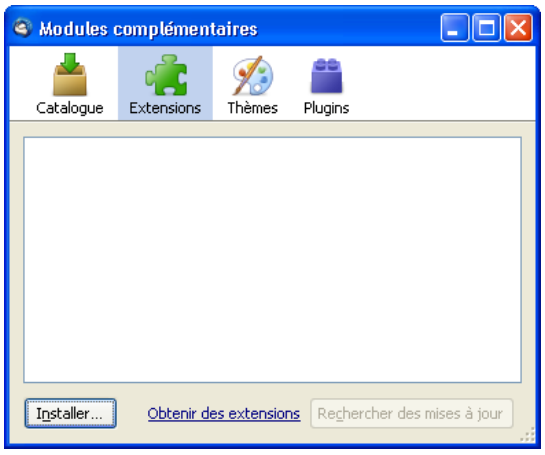


Figure 3: La fenêtre Modules complémentaires affichant le panneau Extensions

Troisième étape. **Cliquez** sur Installer... pour afficher la fenêtre suivante:

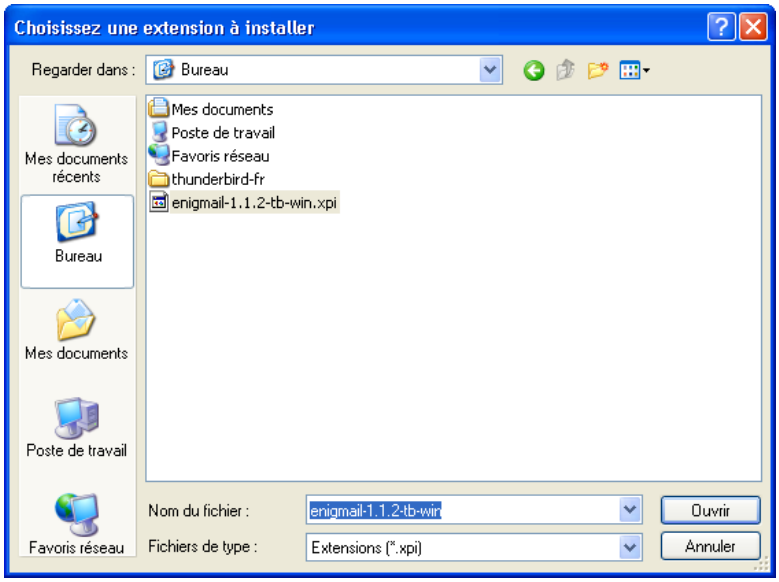


Figure 4: La fenêtre Choisissez une extension à installer

Quatrième étape. Naviguez jusqu'à l'emplacement du dossier où vous avez sauvegardé **Enigmail**, puis **cliquez** sur Ouvrir pour afficher la fenêtre suivante:

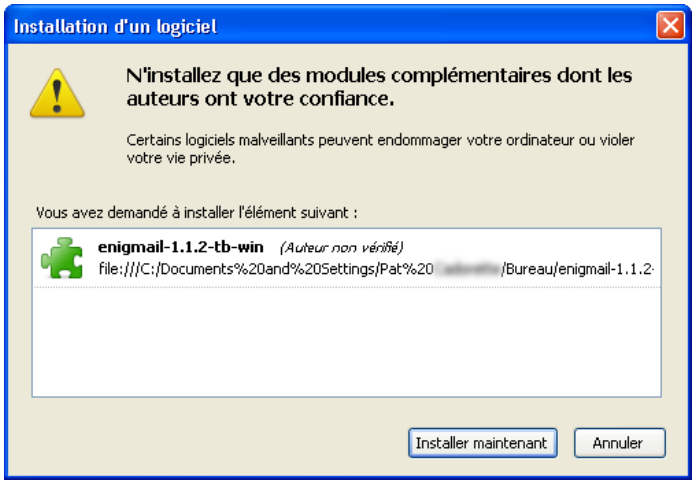

Installation d'un logiciel
N'installez que des modules complémentaires dont les auteurs ont votre confiance.
Certains logiciels malveillants peuvent endommager votre ordinateur ou violer votre vie privée.
Vous avez demandé à installer l'élément suivant :
enigmail-1.1.2-tb-win (Auteur non vérifié)
file:///C:/Documents%20and%20Settings/Pat%20/Bureau/enigmail-1.1.2-
Installer maintenant
Annuler

Figure 5: La fenêtre Installation d'un logiciel

Important: Avant de franchir cette étape, assurez-vous que vos tâches et travaux en ligne aient été sauvegardés!

Cinquième étape. **Cliquez** sur Installer maintenant pour revenir à la *figure 5*, puis **cliquez** sur Redémarrer Thunderbird pour finaliser l'installation du module complémentaire **Enigmail**.

Pour vérifier que l'installation d'**Enigmail** a bien été complétée, retournez à la console **Thunderbird**, et vérifiez si le bouton *OpenPGP* apparaît désormais dans la barre d'outils de **Thunderbird**.

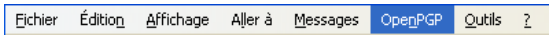


Figure 6: La barre d'outils de Thunderbird avec l'onglet OpenPGP en surbrillance

4.1.3 Comment confirmer qu'Enigmail et GnuPG fonctionnent normalement

Avant de commencer à utiliser **Enigmail** et **GnuPG** pour authentifier et chiffrer vos messages, vous devez d'abord vous assurer que les deux programmes communiquent normalement entre eux.

Première étape. **Sélectionnez OpenPGP > Préférences** pour afficher la fenêtre *Préférences OpenPGP*:

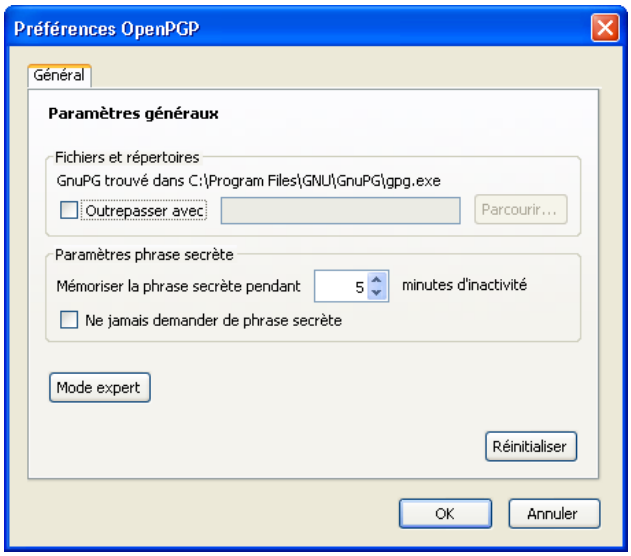


Figure 7: La fenêtre Préférences OpenPGP

Si **GnuPG** a été correctement installé, la ligne GnuPG trouvé dans C:\Program Files\GNU\GnuPG\gpg.exe sera visible dans la section *Fichiers et répertoires*; sinon il est possible que vous receviez un alerte semblable à celle-ci:

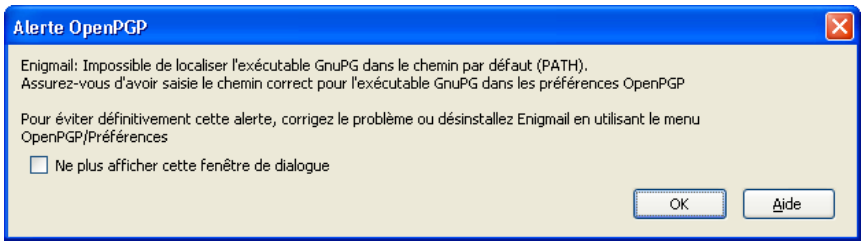

Alerte OpenPGP
Enigmail: Impossible de localiser l'exécutable GnuPG dans le chemin par défaut (PATH).
Assurez-vous d'avoir saisie le chemin correct pour l'exécutable GnuPG dans les préférences OpenPGP
Pour éviter définitivement cette alerte, corrigez le problème ou désinstallez Enigmail en utilisant le menu OpenPGP/Préférences
Ne plus afficher cette fenêtre de dialogue
OK
Aide

Figure 8: Exemple d'alerte OpenPGP

Astuce: Si vous avez reçu un tel message, il est possible que vous ayez installé le fichier au mauvais emplacement. Si tel est le cas, **cochez** l'option *Outrepasser avec* pour activer le bouton *Parcourir*, **cliquez** sur Parcourir... pour activer la fenêtre *Localiser l'agent GnuPG* et naviguer jusqu'à l'emplacement du fichier *gpg.exe* sur votre ordinateur.

Deuxième étape. **Cliquez** sur OK pour retourner à la console **Thunderbird**.

4.2 Comment générer des paires de clés et configurer Enigmail pour qu'il fonctionne avec vos comptes de courriel

Lorsque vous avez confirmé qu'**Enigmail** et **GnuPG** fonctionnent correctement, vous être prêt à configurer un ou plusieurs de vos comptes de courrier électronique afin d'utiliser **Enigmail** pour générer une ou plusieurs paires de clés.

4.2.1 Comment utiliser l'assistant de configuration OpenPGP pour générer une paire de clés

Enigmail offre deux méthodes distinctes pour générer un paire de clés privée/publique; la première consiste à utiliser l'*Assistant de configuration OpenPGP*, et la seconde à employer la fenêtre *Gestion de clefs*.

Pour générer une première paire de clés à l'aide de l'*Assistant de configuration OpenPGP*, veuillez suivre les étapes énumérées ci-dessous:

Première étape. **Sélectionnez OpenPGP > Assistant de configuration** pour ouvrir la fenêtre *Assistant de configuration OpenPGP*:

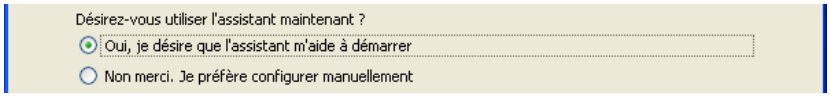

Désirez-vous utiliser l'assistant maintenant ?
Oui, je désire que l'assistant m'aide à démarrer
Non merci. Je préfère configurer manuellement

Figure 9: La fenêtre Assistant de configuration OpenPGP - Bienvenue

Deuxième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

Configurer OpenPGP pour toutes les identités
Oui
Configurer OpenPGP pour les identités suivantes seulement :
Thierry Fictif <thierry.fictif@gmail.com> - thierry.fictif@gmail.com
Thierry Fictif <thierryfictif@riseup.net> - thierryfictif@riseup.net
Note : OpenPGP vérifiera toujours les signatures des messages pour tous les comptes et identités, qu'il y soit actif ou pas.

Figure 10: La fenêtre Sélectionnez une identité

Troisième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

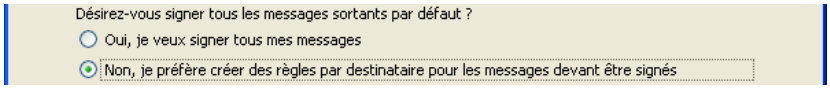

Désirez-vous signer tous les messages sortants par défaut ?
Oui, je veux signer tous mes messages
Non, je préfère créer des règles par destinataire pour les messages devant être signés

Figure 11: La fenêtre Signature - Signer numériquement vos messages sortants

Quatrième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

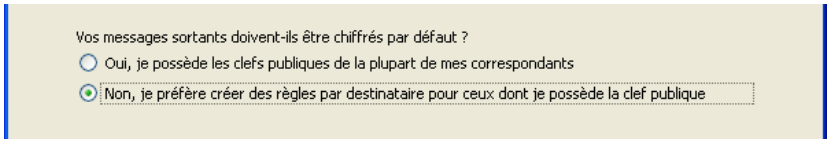

Vos messages sortants doivent-ils être chiffrés par défaut ?
Oui, je possède les clefs publiques de la plupart de mes correspondants
Non, je préfère créer des règles par destinataire pour ceux dont je possède la clef publique

Figure 12: La fenêtre Chiffrement - Chiffrer vos messages sortants

Cinquième étape. **Cliquez** sur Suivant > pour afficher la fenêtre suivante:

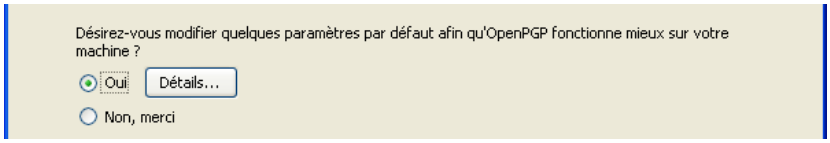

Désirez-vous modifier quelques paramètres par défaut afin qu'OpenPGP fonctionne mieux sur votre machine ?
Oui
Détails...
Non, merci

Figure 13: La fenêtre Désirez-vous modifier quelques paramètres par défaut afin qu'OpenPGP fonctionne mieux sur votre machine?

Sixième étape. **Cliquez** sur Détails... pour afficher la fenêtre suivante:

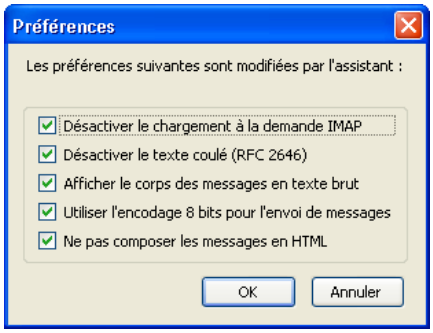

Préférences
Les préférences suivantes sont modifiées par l'assistant :
Désactiver le chargement à la demande IMAP
Désactiver le texte coulé (RFC 2646)
Afficher le corps des messages en texte brut
Utiliser l'encodage 8 bits pour l'envoi de messages
Ne pas composer les messages en HTML
OK
Annuler

Figure 14: La fenêtre Préférences

Commentaire: À la section *3.2 Comment désactiver la fonction HTML dans Thunderbird*, nous avons vu brièvement comment les messages mis en pages en HTML peuvent vous exposer à différentes menaces. Ici, les options *Afficher les corps des messages en texte brut* et *Ne pas composer les messages en HTML* servent précisément à prendre des précautions contre ces menaces.

Septième étape. **Cliquez** sur OK pour revenir à l'*Assistant de configuration OpenPGP*, puis **cliquez** sur Suivant > pour afficher la fenêtre *Créer une clef - Créer une clef pour signer et chiffrer les messages*.

Commentaire: La première fois que créerez une paire de clés, aucun de vos comptes de courriel n'apparaîtra dans la liste défilante.

Huitième étape. **Saisissez** un mot de passe complexe (ou phrase secrète) d'au moins 8 caractères alphanumériques dans les deux champs *Phrase secrète*:

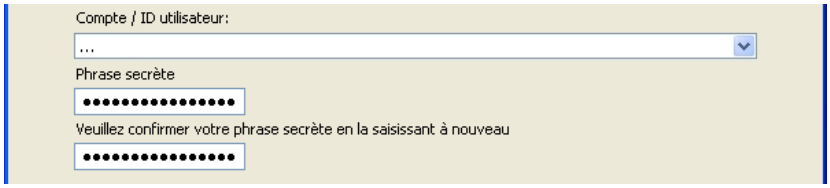


Figure 15: La fenêtre Créer une clef - Créer une clef pour signer et chiffrer les messages

Neuvième étape. **Cliquez** sur Suivant > pour confirmer ces réglages, puis **cliquez** sur < Précédent pour retourner à la fenêtre *Créer un clef*; le nom de votre premier compte de courriel devrait maintenant être affiché, comme suit:

Compte / ID utilisateur:
Thierry Fictif <thierryfictif@riseup.net> - thierryfictif@riseup.net

Figure 16: Le Compte /ID utilisateur nouvellement créé

Dixième étape. **Cliquez** sur Suivant > pour afficher la fenêtre *Résumé*, qui devrait être fidèle aux réglages utilisés lors de la création de la paire de clés.

Commentaire: Chaque paire de clés générée avec l'*Assistant de configuration OpenPGP* est automatiquement basée sur une structure 2048-bit et a une durée de vie de 5 ans. Ces deux caractéristiques ne peuvent pas être modifiées après la création d'une paire de clés à l'aide de cette méthode.

4.2.2 Comment générer une paire de clés et un certificat de révocation supplémentaires pour un autre compte de courriel

Il est de pratique courante de conserver une paire de clés distincte pour chaque compte de courriel. Suivez les étapes énumérées ci-dessous pour générer des paires de clés supplémentaires pour vos autres comptes. La création d'une paire de clés implique également la création d'un *certificat de révocation* qui lui est associé. Envoyez ce certificat à vos contacts pour leur permettre de désactiver votre clé publique dans l'éventualité où votre clé privée serait compromise ou perdue.

Première étape. **Sélectionnez OpenPGP > Gestion de clefs** pour afficher la fenêtre suivante:

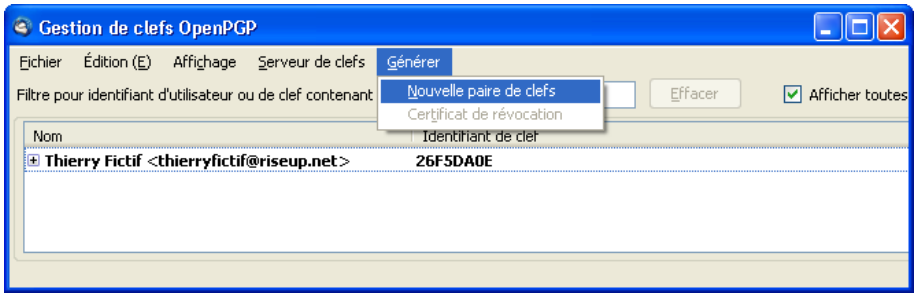


Figure 17: Le menu Générer du gestionnaire de clefs OpenPGP Key avec l'option Nouvelle paire de clefs sélectionnée

Commentaire: **Cochez** l'option *Afficher toutes les clefs par défaut* pour afficher la paire de clés générée à l'aide de l'*Assistant de configuration OpenPGP* pour votre premier compte de courriel, tel qu'illustré à la *figure 17* ci-dessus.

Deuxième étape. **Sélectionnez Générer > Nouvelle paire de clefs** dans la fenêtre de *gestion de clefs*, tel qu'illustré à la *figure 20* ci-dessus, pour afficher la fenêtre suivante:

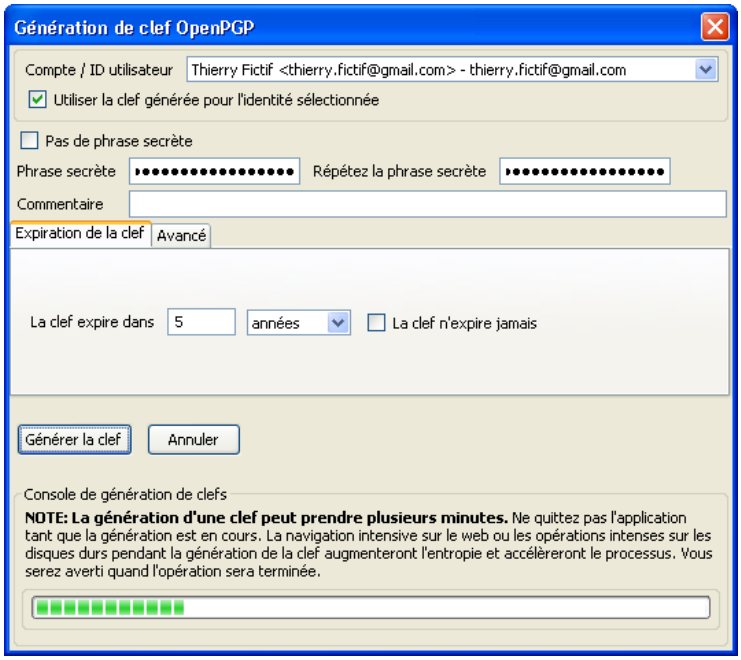

Génération de clef OpenPGP
Compte / ID utilisateur
Thierry Fictif <thierry.fictif@gmail.com> - thierry.fictif@gmail.com
Utiliser la clef générée pour l'identité sélectionnée
Pas de phrase secrète
Phrase secrète
Répétez la phrase secrète
Commentaire
Expiration de la clef
Avancé
La clef expire dans
5
années
La clef n'expire jamais
Générer la clef
Annuler
Console de génération de clefs
NOTE: La génération d'une clef peut prendre plusieurs minutes. Ne quittez pas l'application tant que la génération est en cours. La navigation intensive sur le web ou les opérations intenses sur les disques durs pendant la génération de la clef augmenteront l'entropie et accélèreront le processus. Vous serez averti quand l'opération sera terminée.

Figure 18: La fenêtre Génération de clefs OpenPGP

Troisième étape. **Sélectionnez** un compte de courrier électronique dans la liste défilante *Compte / ID utilisateur*, puis **cochez** l'option *Utiliser la clef générée pour l'identité sélectionnée*. Créez ensuite une phrase secrète pour protéger votre clé privée.

Commentaire: Comme son nom l'indique, une phrase secrète est en quelque sorte un mot de passe long et complexe. **Enigmail** vous demande de choisir un mot de passe qui est plus long et plus complexe que d'habitude.

Important: Il faut *toujours* générer une paire de clés avec une phrase secrète, et ne *jamais* activer l'option 'Pas de phrase secrète'.

Figure 19: La fenêtre Génération de clef OpenPGP affichant l'onglet Expiration de la clef

Commentaire: La durée de vie d'une paire de clés dépend uniquement de vos besoins en matière de confidentialité et de sécurité. Plus vous changez fréquemment de paires de clés, plus il est difficile pour une tierce partie de compromettre votre nouvelle paire de clés. Par contre, chaque fois que vous changez de paire de clés, vous devez l'envoyer à vos correspondants et recommencer la vérification.

Cinquième étape. **Saisissez** le nombre approprié, puis **sélectionnez** l'unité de temps désiré (*jours*, *mois* ou *années*) pour déterminer la durée de vie de la paire de clés.

Sixième étape. **Cliquez** sur Générer la clef pour afficher la fenêtre suivante:

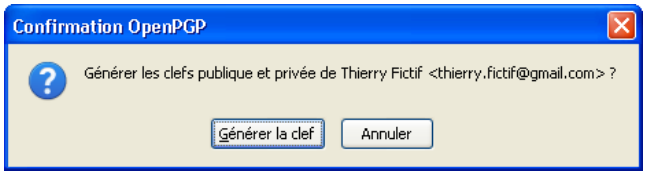


Figure 20: La boîte de dialogue de Confirmation OpenPGP

Septième étape. **Cliquez** sur Générer la clef pour afficher la fenêtre suivante:

Confirmation OpenPGP
Génération de la clef terminée! L'identifiant <thierry.fictif@gmail.com> sera utilisé pour la signature.
Il est grandement recommandé de créer un certificat de révocation pour la clef. Ce certificat peut être utilisé pour invalider votre clef dans le cas où votre clef privée soit perdue ou compromise.
Désirez-vous créer un certificat de révocation maintenant ?
Générer le certificat
Annuler

Figure 21: La boîte de dialogue de Confirmation OpenPGP

Huitième étape. **Cliquez** sur Générer le certificat pour afficher la fenêtre de navigation *Créer et enregistrer le certificat de révocation*.

Commentaire: Si avez connaissance qu'une tierce partie hostile ou malveillante est parvenu à accéder sans autorisation à votre clé publique, ou que vous avez vous-même perdu l'accès, vous pouvez envoyer un certificat de révocation à vos contacts pour les informer qu'ils ne doivent plus utiliser votre clé publique. Soyez aussi conscient que vous devrez mener cette opération si votre ordinateur est perdu, volé ou confisqué. Il est fortement recommandé de faire une copie de sauvegarde sécurisée de votre certificat de révocation.

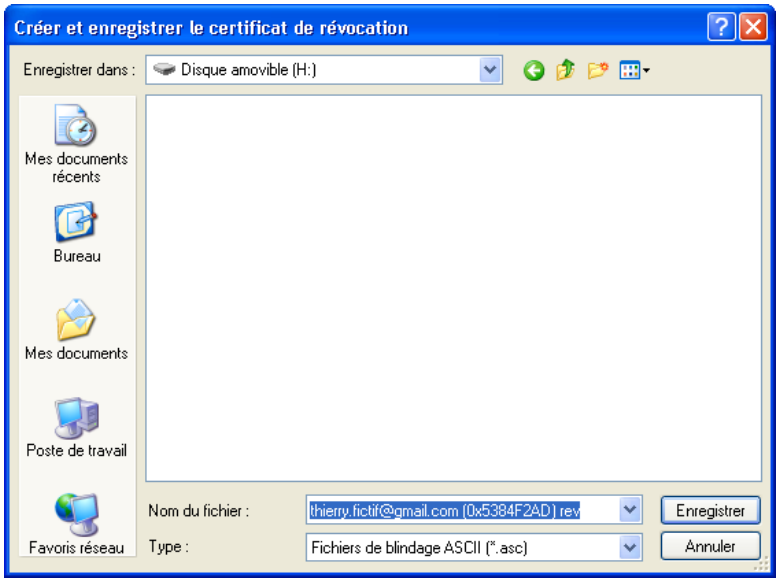


Figure 22: La fenêtre Créer et enregistrer le certificat de révocation

Neuvième étape. **Cliquez** sur Enregistrer pour afficher la fenêtre suivante; puis **saisissez** la phrase secrète associée à ce compte:

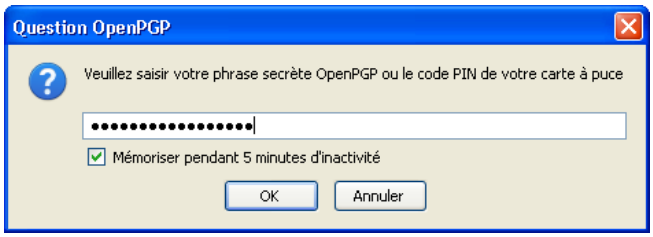

Question OpenPGP
Veuillez saisir votre phrase secrète OpenPGP ou le code PIN de votre carte à puce
Mémoriser pendant 5 minutes d'inactivité
OK
Annuler

Figure 23: La fenêtre Veuillez saisir votre phrase secrète OpenPGP

Dixième étape. **Cliquez** sur OK pour finaliser la génération de la paire de clés et du certificat de révocation, et revenir à la fenêtre suivante:

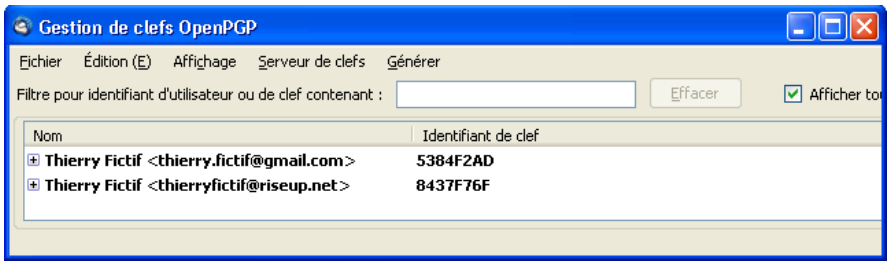


Figure 24: La fenêtre Gestion de clefs OpenPGP affichant la nouvelle paire de clés

Commentaire: **Cochez** l'option *Afficher toutes les clefs par défaut* pour afficher toutes les clés avec leur compte respectif, si vous êtes seul et dans un milieu sûr.

Maintenant que vous avez générer une paire de clés et un certificat de révocation, vous êtes prêt à échanger vos clés publiques avec un correspondant de confiance.

4.2.3 Comment configurer Enigmail pour une utilisation avec votre compte de courrier électronique

Pour activer l'utilisation d'**Enigmail** avec un compte en particulier, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez Outils > Paramètres des comptes**.

Deuxième étape. **Sélectionnez** l'item de menu *OpenPGP* dans l'encadré de gauche, tel qu'illustré ci-dessous:

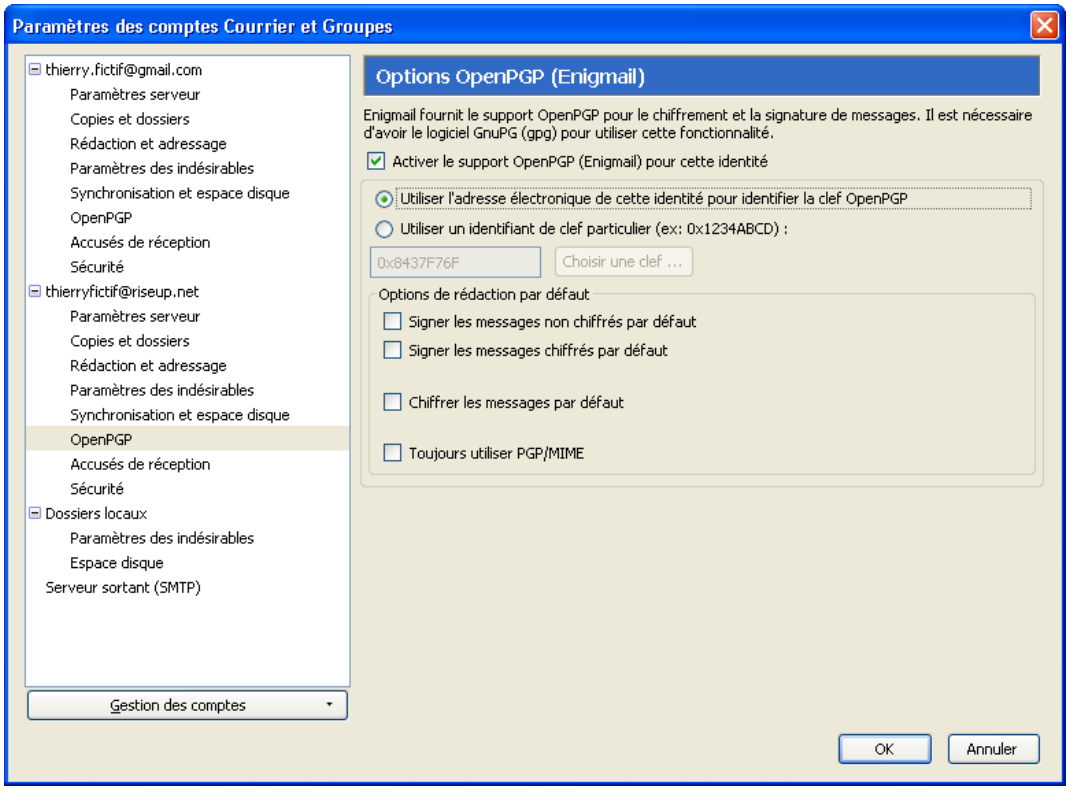


Figure 25: La fenêtre Paramètres des comptes - OpenPGP

Troisième étape. **Cochez** l'option *Activer le support OpenPGP (Enigmail) pour cette identité* et **sélectionnez** l'option *Utiliser l'adresse électronique de cette identité pour identifier la clef OpenPGP*, tel qu'illustré ci-dessus à la *figure 25*.

Quatrième étape. **Cliquez** sur OK pour revenir à la console **Thunderbird**.

4.3 Comment échanger vos clés publiques

Avant de commencer à envoyer et recevoir des messages chiffré, vous et vos correspondants devez échanger vos clés publiques. Vous devez également confirmer la validité des clés que vous acceptez en vous assurant qu'elles appartiennent bel et bien aux expéditeurs qui sont censées vous les avoir envoyées.

4.3.1 Comment envoyer une clé publique avec Enigmail

Pour envoyer une clé publique en utilisant **Enigmail/OpenPGP**, vous et votre correspondant devez suivre les étapes énumérées ci-dessous:

Première étape. **Ouvrez Thunderbird**, puis **cliquez** sur

pour rédiger un nouveau message.

Deuxième étape. **Cliquez** sur

OU **sélectionnez Fichier > Joindre > Fichier(s)** pour afficher la fenêtre to *Joindre les fichiers*, naviguez jusqu'à l'emplacement de votre clé publique, puis **cliquez** sur

pour joindre votre clé publique. La fenêtre de rédaction devrait maintenant ressembler à ceci:

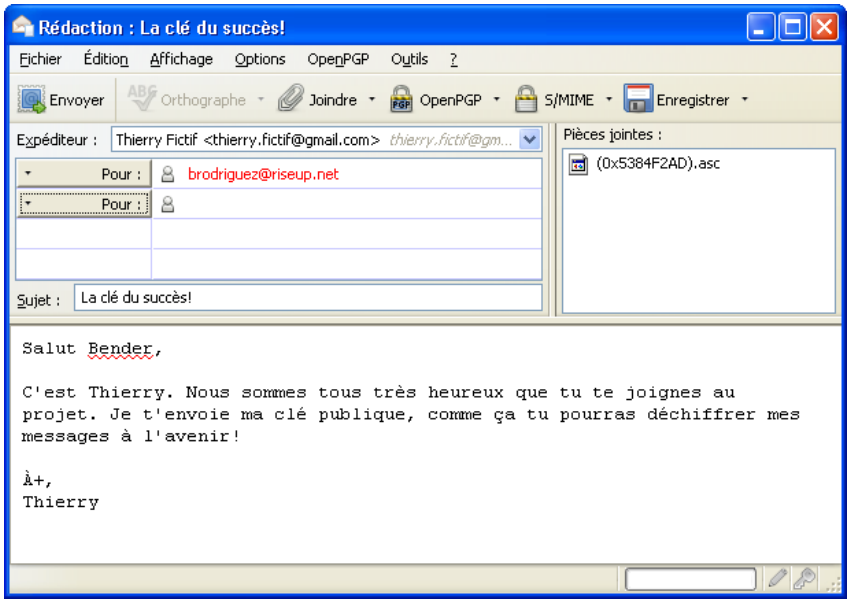

Rédaction : La clé du succès!
Fichier Édition Affichage Options OpenPGP Outils ?
Envoyer Orthographe Joindre OpenPGP S/MIME Enregistrer
Expéditeur : Thierry Fictif <thierry.fictif@gmail.com>
Pour : brodriguez@riseup.net
Pour :
Sujet : La clé du succès!
Pièces jointes :
(0x5384F2AD).asc
Salut Bender,
C'est Thierry. Nous sommes tous très heureux que tu te joignes au projet. Je t'envoie ma clé publique, comme ça tu pourras déchiffrer mes messages à l'avenir!
À+,
Thierry

Figure 26: La fenêtre de rédaction d'un message affichant la clé publique dans le panneau des pièces jointes

Commentaire: Vous pouvez également joindre votre clé publique en sélectionnant **OpenPGP > Attacher ma clef publique**. Par contre, cette méthode n'affiche pas la clé dans le panneau *pièces jointes*:; la clé s'affichera plutôt au bas du message que recevra votre correspondant, comme dans l'exemple ci-dessous:

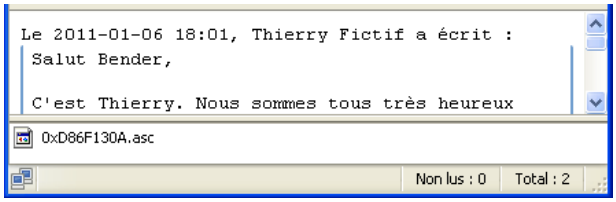

Le 2011-01-06 18:01, Thierry Fictif a écrit :
Salut Bender,
C'est Thierry. Nous sommes tous très heureux
0xD86F130A.asc
Non lus : 0
Total : 2

Figure 27: Un exemple de clé publique jointe à un message par l'item Attacher ma clef publique du menu OpenPGP

Troisième étape. **Cliquez** sur

pour envoyer votre message, avec votre clé publique jointe, pour afficher la fenêtre suivante:

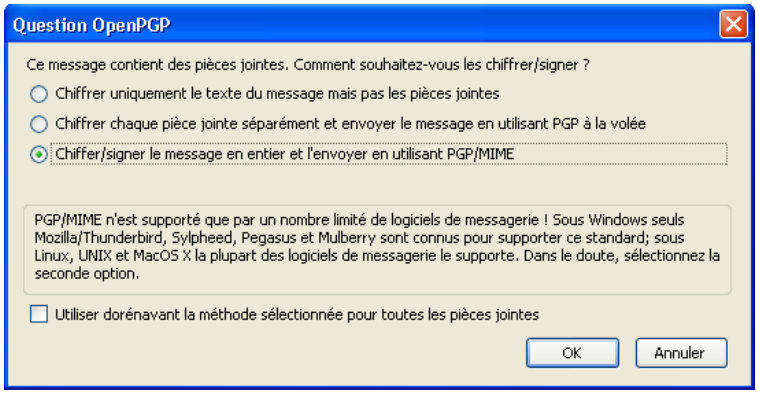

Question OpenPGP
Ce message contient des pièces jointes. Comment souhaitez-vous les chiffrer/signer ?
Chiffrer uniquement le texte du message mais pas les pièces jointes
Chiffrer chaque pièce jointe séparément et envoyer le message en utilisant PGP à la volée
Chiffer/signer le message en entier et l'envoyer en utilisant PGP/MIME
PGP/MIME n'est supporté que par un nombre limité de logiciels de messagerie ! Sous Windows seuls Mozilla/Thunderbird, Sylpheed, Pegasus et Mulberry sont connus pour supporter ce standard; sous Linux, UNIX et MacOS X la plupart des logiciels de messagerie le supporte. Dans le doute, sélectionnez la seconde option.
Utiliser dorénavant la méthode sélectionnée pour toutes les pièces jointes
OK
Annuler

Figure 28: La fenêtre d'invite de OpenPGP servant à définir le mode de chiffrement et de signature par défaut

Quatrième étape. **Cochez** l'option *Chiffrer/signer le message en entier*, puis **cliquez** sur OK pour afficher la fenêtre d'invite illustrée à la *figure 23*.

Cinquième étape. **Saisissez** votre phrase secrète, puis **cliquez** sur OK pour afficher la fenêtre suivante:

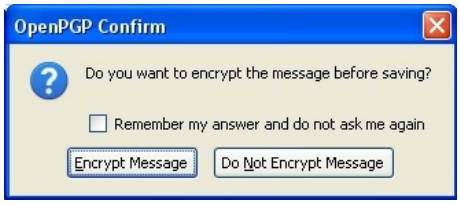

OpenPGP Confirm
Do you want to encrypt the message before saving?
Remember my answer and do not ask me again
Encrypt Message
Do Not Encrypt Message

Figure 29: La fenêtre d'invite d'OpenPGP - Do you want to encrypt the message before saving screen

Sixième étape. **Cliquez** sur Encrypt Message pour chiffrer, signer et envoyer votre message.

4.3.2 Comment importer une clé publique avec Enigmail

Vous et votre correspondant devrez suivre les étapes énumérées ci-dessous pour importer la clé publique de l'autre:

Première étape. **Sélectionnez** et **ouvrez** le message qui contient la clé publique de votre correspondant.

Si la clé publique de votre correspondant est incorporée au message, le bouton *Déchiffrer* sera activé et l'en-tête suivante s'affichera dans le panneau du message:

Figure 30: Le message Cliquez sur le bouton 'Déchiffrer' pour importer la clef publique jointe au message

Deuxième étape. **Cliquez** sur Decrypt pour lancer automatiquement le balayage du message reçu pour détecter des données chiffrées. Lorsqu'*Enigmail/OpenPGP* détecte un message contenant une clé publique, il vous demande d'importer la clé comme suit:

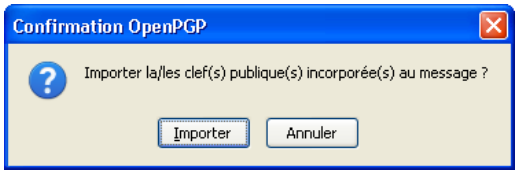


Figure 31: L'invite de confirmation OpenPGP Importer la/les clef(s) publique(s) incorporée(s) au message?

Troisième étape. **Cliquez** sur Importer pour importer la clé publique de votre correspondant.

Si vous avez réussi à importer la clé publique, un message semblable à celui-ci s'affichera:

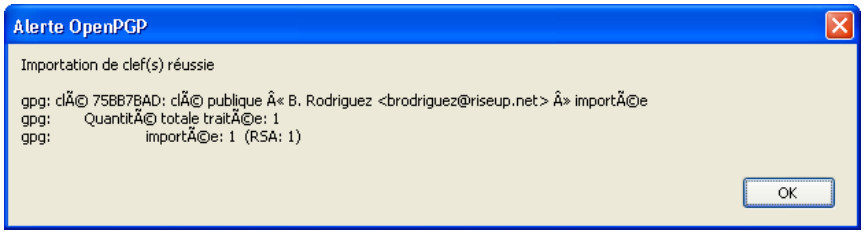

Alerte OpenPGP
Importation de clef(s) réussie
gpg: clÃ© 75BB7BAD: clÃ© publique Â« B. Rodriguez <brodriguez@riseup.net> Â» importÃ©e
gpg: QuantitÃ© totale traitÃ©e: 1
gpg: importÃ©e: 1 (RSA: 1)
OK

Figure 32: Une fenêtre d'alerte OpenPGP affichant la clé publique de votre correspondant

Pour confirmer que vous avez reçu la clé publique de votre correspondant, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez OpenPGP > Gestion de clefs** pour afficher la fenêtre *Gestion de clefs OpenPGP*:

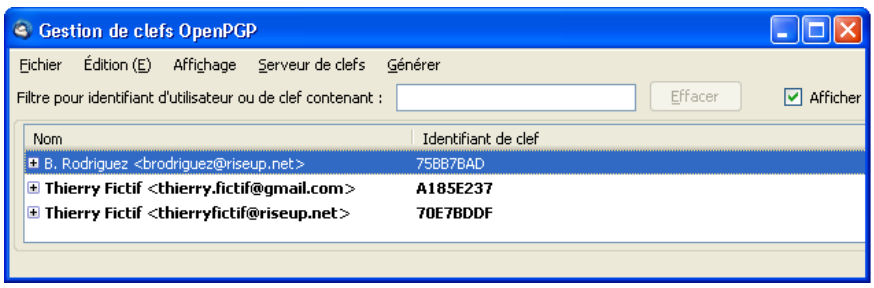


Figure 33: La fenêtre OpenPGP - Gestion de clefs affichant la clé publique récemment importée

4.4 Comment valider et signer un paire de clés

Finalement, vous devez vérifier que la clé importée appartient bel et bien à la personne censée vous l'avoir envoyée, et confimrer sa 'validité'. C'est une étape importante que vous et vos contacts devrez suivre pour chaque clé publique que vous recevez.

4.4.1 Comment valider une paire de clés

Première étape. **Contactez** votre correspondant par un autre moyen de communication que le courrier électronique. Vous pouvez utiliser le téléphone, le message texte, You can use a telephone, text messages, la **Voix sur réseau IP** (**VoIP**) ou toute autre méthode, mais vous **devez** être absolument certain que vous communiquez avec la bonne personne. À cet égard, les conversations téléphonique ou les rencontres en face à face sont les meilleures solutions possibles, si vous êtes en mesure de le faire.

Deuxième étape. Vous et votre correspondant devez vérifier l'empreinte des clés publiques que vous avez échangées. Une empreinte est une série unique de chiffres et de lettres qui sert à identifier chaque clé. Vous pouvez utiliser la fenêtre de *Gestion de clefs* d'**OpenPGP** pour visualiser l'empreinte des paires de clés que vous avez créées et des clés publiques que vous avez importées.

Pour visualiser l'empreinte d'une paire de clés en particulier, suivez les étapes énumérées ci-dessous:

Première étape. **Sélectionnez > OpenPGP > Gestion de clefs**, puis **cliquez à droite** sur la clé dont vous voulez vérifier l'empreinte pour afficher le menu contextuel suivant:

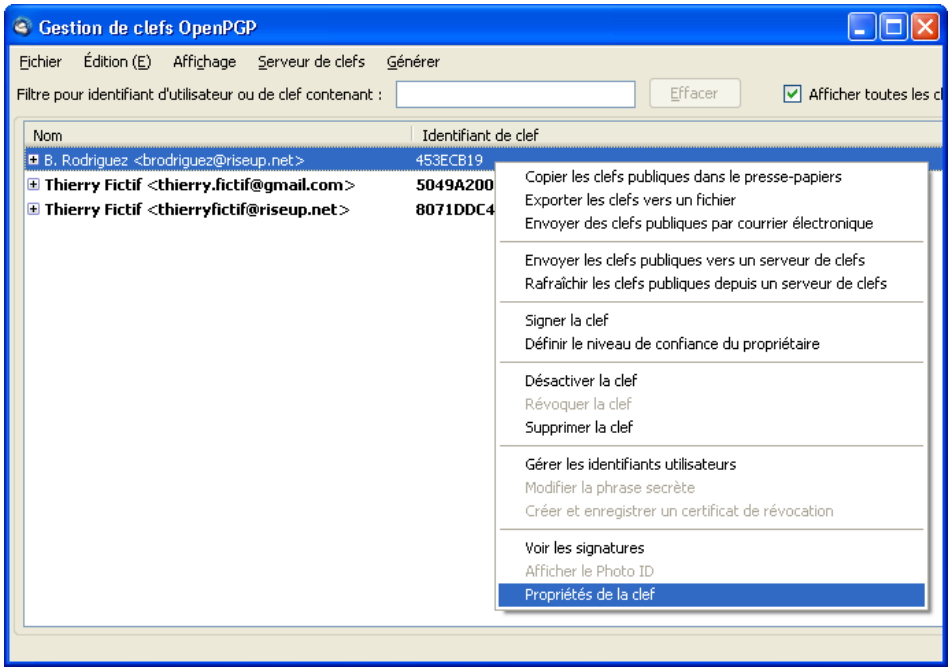


Figure 34: Le menu contextuel de Gestion de clefs d'OpenPGP avec l'item Propriétés de la clef sélectionné

Deuxième étape. **Sélectionnez** l'item *Propriété de la clef* pour afficher la fenêtre suivante:

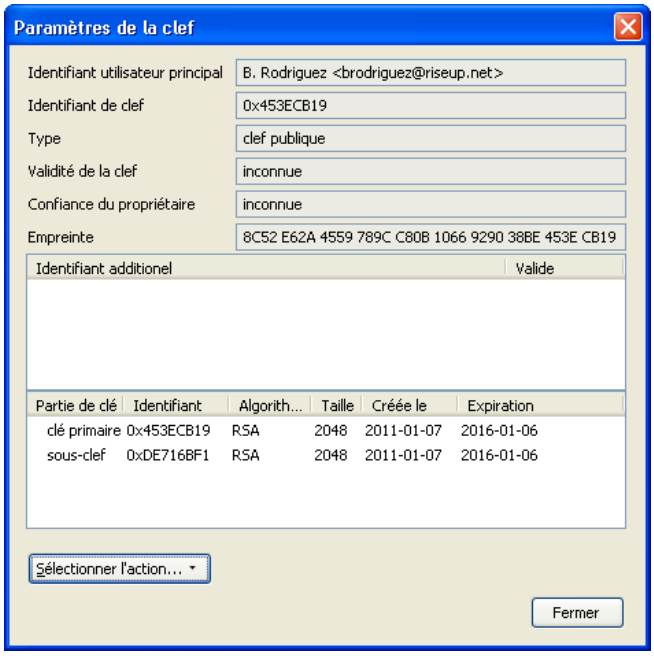


Figure 35: La fenêtre Propriétés de la clef

Votre correspondant devrait suivre les mêmes étapes. Confirmez l'un auprès de l'autre que l'empreinte des clés que vous

avez correspond bel et bien à l'original. Si les empreintes ne correspondent pas, échangez vos clés publiques à nouveau et répétez le processus de validation.

Commentaire: L'empreinte elle-même n'est pas secrète et peut être enregistrée quelque part en vue d'une vérification ultérieure.

4.4.2 Comment signer une clé publique validée

Lorsque vous avez déterminé que la clé publique d'un correspondant donné est valide, vous devez la *signer* pour confirmer que vous considérez cette clé comme valide.

Pour signer une clé publique validée, suivez les étapes énumérées ci-dessous:

Première étape. **Cliquez** sur OK pour revenir à la fenêtre *Gestion de clefs*

Deuxième étape. **Cliquez à droite** sur la clé publique de votre correspondant, puis **sélectionnez** l'item *Signer la clef* dans le menu contextuel pour afficher la fenêtre suivante:

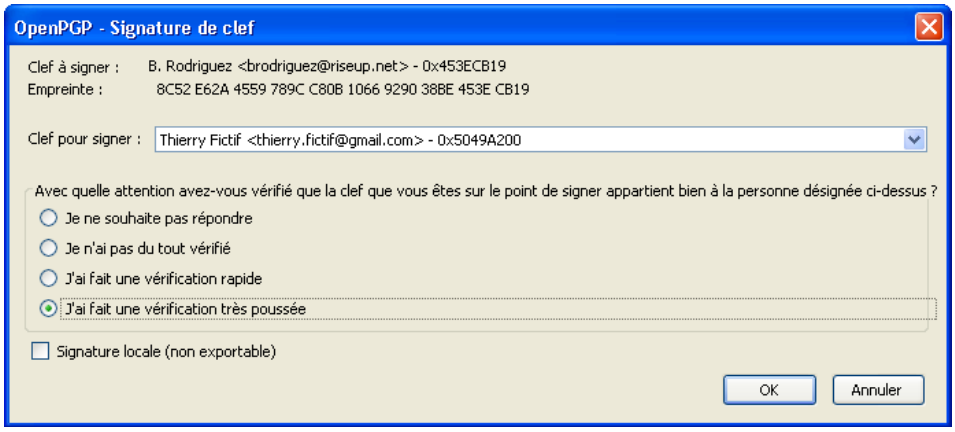


Figure 36: La fenêtre OpenPGP - Signature de la clef

Troisième étape. **Cochez** l'option *J'ai fait une vérification très poussée*, puis **cliquez** sur OK pour compléter la signature de la clé publique de votre correspondant, finaliser le processus de validation et revenir à la fenêtre *Gestion de clefs OpenPGP*:

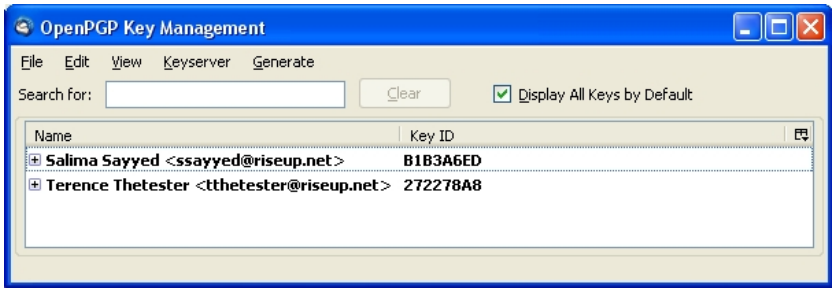


Figure 37: La fenêtre Gestion de clefs OpenPGP affichant la paire de clés validée

4.4.3 COmment gérer vos paires de clés

La fenêtre *Gestion de clefs OpenPGP* est utilisée pour générer, valider et signer différentes paires de clés. Il vous est aussi possible de mener d'autres tâches de gestion, y compris:

- **Modifier la phrase secrète**: Cette fonction vous permet de changer la phrase secrète qui protège votre paire de clés.
- **Gérer les identifiants utilisateurs**: Cette fonction vous permet d'associer plus d'un compte de courriel à une paire de clés donnée.
- **Créer et enregistrer un certificat de révocation**: Cette fonction vous permet de générer un nouveau certificat de révocation si vous avez perdu celui que vous aviez créé à l'origine.

4.5 Comment chiffrer et déchiffrer des messages

Important: L'en-tête d'un message de courrier électronique, c'est-à-dire le *Sujet* et les destinataires (y compris tous les renseignements inclus dans les champs *Pour*, *CC* et *BCC*), *ne peut pas* être chiffrée et sera envoyée en clair. Pour préserver la confidentialité et la sécurité de vos communications par courriel, le sujet ou le titre de vos messages devraient être vague et non descriptifs pour éviter de révéler des renseignements sensibles. De plus, il est fortement recommandé de mettre toutes les adresses de vos destinataires dans le champs *BCC* lorsque vous envoyez des messages à un groupe de personnes.

Lorsque vous chiffrez des messages avec des pièces jointes, il est fortement recommandé d'utiliser l'option **PGP/MIME**, puisque ceci étendra le chiffrement aux fichiers joints au message.

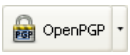
4.5.1 Comment chiffrer un message

Une fois que vous et votre correspondant avez tous deux importé, validé et signé vos clés publiques respectives, vous êtes désormais prêts à envoyer des messages chiffrés et à déchiffrer ceux que l'on vous envoie.

Pour chiffrer le contenu d'un message, suivez les étapes énumérées ci-dessous:

Première étape. **Ouvrez** votre compte de courriel et **cliquez** sur

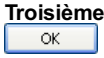
pour rédiger un nouveau message.

Deuxième étape. **Cliquez** sur 

pour afficher la fenêtre suivante:

Figure 38: La fenêtre Chiffrement OpenPGP

Commentaire: Si vous avez coché l'option *Chiffrer/signer le message en entier et l'envoyer en utilisant* ***PGP/MIME*** à la *figure 28* tel qu'indiqué, la *figure 38* ne s'affichera pas.

Troisième étape. **Cochez** les options *Signer le message* et *Chiffrer le message* tel qu'illustré à la *figure 38*, puis **cliquez** sur 

pour finaliser la signature et le chiffrement de votre message.

Commentaire: Pour vérifier que votre message sera bel et bien chiffré et signé, assurez-vous que les deux icones ci-dessous figurent dan sle coin inférieur droit du panneau de message:

Figure 39: Les icones de confirmation de la signature et du chiffrement

Quatrième étape. **Cliquez** sur

pour envoyer le message. Une fenêtre d'invite vous demande de saisir votre phrase secrète pour utiliser votre clé privée et signer le message.

4.5.2 Comment déchiffrer un message

Lorsque vous recevez un message chiffré, **Enigmail/OpenPGP** tentera automatiquement de le déchiffrer sur réception ou lorsque vous souuhaitez l'ouvrir. La fenêtre suivante s'affiche:

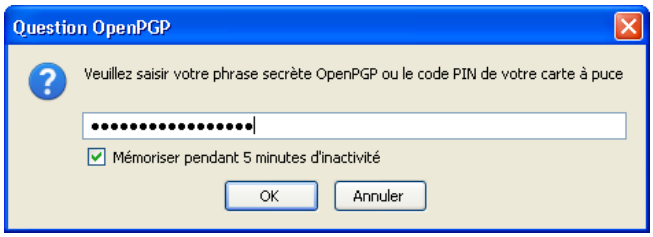

Question OpenPGP
Veuillez saisir votre phrase secrète OpenPGP ou le code PIN de votre carte à puce
Mémoriser pendant 5 minutes d'inactivité
OK
Annuler

Figure 40: La fenêtre d'invite d'OpenPGP - Veuillez saisir votre phrase secrète OpnePGP ou le code PIN de votre carte à puce

Première étape. **Saisissez** votre phrase secrète tel qu'illustré à la *figure 40*.

Lorsque vous avez saisi la phrase secrète de votre clé privée, le message est déchiffré et affiché en clair:

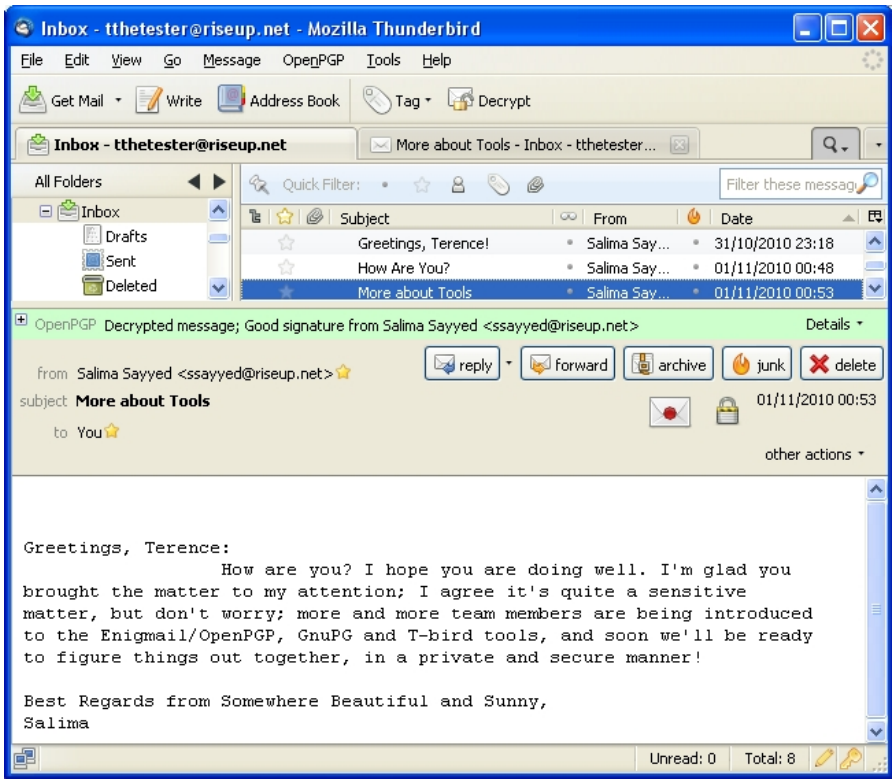

Inbox - tthetester@riseup.net - Mozilla Thunderbird
File Edit View Go Message OpenPGP Tools Help
Get Mail Write Address Book Tag Decrypt
Inbox - tthetester@riseup.net
More about Tools - Inbox - tthetester...
All Folders
Inbox
Drafts
Sent
Deleted
Quick Filter:
Filter these messag
Subject From Date
Greetings, Terence! Salima Say... 31/10/2010 23:18
How Are You? Salima Say... 01/11/2010 00:48
More about Tools Salima Say... 01/11/2010 00:53
OpenPGP Decrypted message; Good signature from Salima Sayyed <ssayyed@riseup.net>
Details
reply forward archive junk delete
from Salima Sayyed <ssayyed@riseup.net>
subject More about Tools
to You
01/11/2010 00:53
other actions
Greetings, Terence:
How are you? I hope you are doing well. I'm glad you
brought the matter to my attention; I agree it's quite a sensitive
matter, but don't worry; more and more team members are being introduced
to the Enigmail/OpenPGP, GnuPG and T-bird tools, and soon we'll be ready
to figure things out together, in a private and secure manner!
Best Regards from Somewhere Beautiful and Sunny,
Salima
Unread: 0
Total: 8

Figure 41: Le message déchiffré dans le panneau de message

Vous avez réussi à déchiffrer le message. En répétant les étapes énumérées à la section **4.5 Comment chiffrer et déchiffrer des messages** chaque fois que votre correspondant et vous échangez des messages, vous maintiendrez une voie de communication privée et sécurisée, même si des tierces parties essaient de surveiller vos communications.

Faq et questions récapitulatives

5.0 Faq et questions récapitulatives

Claudia et Pablo ont configuré **Mozilla Thunderbird** pour envoyer et recevoir des messages avec leurs comptes **RiseUp**. Après avoir consulté leur courrier, ils ont été ravis de pouvoir poursuivre leur lecture des messages même après s'être déconnecté d'Internet.

Peu après, Claudia et Pablo ont installé **GnuPG** et **Enigmail**, créé leurs propres paires de clés, échangé leurs clés publiques et validé respectivement leurs clés en comparant leurs empreintes.

Même s'il leur a fallu un certain temps pour comprendre les complexités du chiffrement asymétrique (par clé publique), ils peuvent d'ores et déjà envisager les avantages que comportent un moyen de communication chiffré et sécurisé. Cependant, comme avec n'importe quel nouveau logiciel, ils ont encore quelques questions.

***Q**: Que se passe t-il si je n'installe qu'**Enigmail**, et pas **GnuPG**?*

***A**: C'est simple. **Enigmail** ne fonctionnera tout simplement pas. En fait, c'est le logiciel **GnuPG** qui fournit le moteur de chiffrement utilisé par **Enigmail**.*

***Q**: Combien de comptes de courrier électronique différents puis-je enregistrer dans **Thunderbird**?*

***A**: Autant que tu le désires! **Thunderbird** peut facilement gérer 20 comptes de courrier électronique, ou même plus! ** **Q**: Mon ami a un compte Gmail. Devrais-je essayer de le convaincre d'installer **Thunderbird**, **Enigmail** et **GnuPG**?*

***A**: Ce serait idéal. Il n'a qu'à s'assurer de régler ses paramètres de sécurité exactement comme tu l'as fait toi-même. Après cela, vous disposerez d'un moyen extrêmement efficace de communiquer de façon sûre et confidentielle!*

***Q**:Rappelle-moi encore, quelle partie du message est chiffrée par **Enigmail**?*

***A**: **Enigmail** chiffre le contenu du message. Il ne chiffre pas la ligne du sujet, ni l'adresse de courriel ou le nom que tu as choisi d'associer à ce compte de courriel. Si tu veux envoyer un message confidentiel, assure-toi que la ligne du sujet ne te trahit pas! Et si tu souhaites rester anonyme, évite d'utiliser ton vrai nom lorsque tu crées ton compte de courriel.*

***Q**: Je ne saisis toujours pas le but d'apposer une signature numérique à mes messages.*

***A**: Une signature numérique prouve que tu est bel et bien l'expéditeur d'un message donné, et que ce message n'a pas été modifié ou piraté entre le moment où tu l'as expédié et celui où ton destinataire l'a reçu. C'est un peu comme un cachet de cire utilisé pour sceller une lettre importante.*

5.1 Questions récapitulatives

- Avant de pouvoir envoyer un message chiffré à un de vos collègues, quels logiciels devez-vous d'abord installer et configurer?
- Comment pouvez-vous accéder à vos messages de façon sûre en utilisant **Thunderbird**?

- Comment pouvez-vous stocker les mots de passe de vos comptes de courriel en utilisant **Thunderbird**?
- Comment pouvez-vous vous protéger contre des messages comportant du contenu malveillant?
- Quelle est la différence entre accéder à vos courriels par l'intermédiaire d'un navigateur Web, et y accéder avec un client de messagerie comme Thunderbird?

Firefox - navigateur Internet

Mozilla Firefox est un navigateur Internet gratuit et de plus en plus populaire. Sa fonctionnalité est améliorée par l'inclusion de nombreux modules complémentaires, dont ceux qui augmentent le degré de confidentialité et la sécurité du navigateur.

Site Internet

www.mozilla.com/firefox [160]

Configuration requise :

- Compatible avec toutes les versions de Windows

Versions utilisées pour rédiger ce guide :

- Firefox 3.0.4
- NoScript 1.9.1
- FormFox 1.6.3
- McAfee Site Advisor 28.0
- PetName 1.6
- FireGPG 0.7.5

Licence :

- FLOSS (Free/Libre Open Source Software)

Pour installer Firefox

- *Lisez la courte introduction des Guides pratiques [13]*
- ***Cliquez sur l'icône de Firefox ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.*
- ***Cliquez sur l'icône de NoScript** et sauvegardez le fichier de l'extension.*
- ***Optionnel : cliquez sur les autres icônes** et sauvegardez les fichiers d'extension.*
- *Poursuivez la lecture du guide pratique et installez NoScript et les autres modules complémentaires aux sections 4 et 5.*
- *Si vous avez sauvegardé les exécutables et les fichiers d'extension sur votre ordinateur, vous pouvez les supprimer après l'installation.*

Firefox: [161] **NoScript**: [162] **FormFox**: [163] **Petname**: [164] **FireGPG**: [165]

Niveau : 1 : Débutant, **2 : Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

Temps d'apprentissage : 20 - 30 minutes

Ce que vous apportera l'utilisation de cet outil :

- Un navigateur Web stable et sûr, dont la fonctionnalité peut être améliorée par de nombreux modules complémentaires;
- La capacité de vous protéger contre des programmes potentiellement dangereux et des sites Internet malveillants;
- La capacité d'effacer de votre ordinateur les traces de vos séances de navigation sur Internet.

1.1 À propos de cet outil

Dans ce guide, nous tenons pour acquis que vous savez déjà utiliser un navigateur Web; ce guide n'explique pas comment utiliser les fonctions de base du navigateur Firefox. Nous y exposons plutôt quelques uns des modules complémentaires qui contribuent à améliorer la fonctionnalité et la sécurité de Firefox.

Les modules complémentaires de Mozilla sont conçus tout spécialement pour le navigateur Web Firefox. Les *modules complémentaires* (ou *plugins*, *extensions* et parfois *greffons*), sont des petits programmes qui ajoutent des fonctions ou améliorent les fonctions existantes d'une application particulière, dans ce cas-ci, Firefox.

Dans ce guide, vous apprendrez à télécharger, installer et utiliser les modules complémentaires Mozilla listés ci-dessous, afin d'améliorer le niveau de confidentialité et de sécurité de votre navigateur Web Firefox et de votre expérience de navigation en général.

Le module complémentaire **NoScript** est documenté séparément à la section **4.0 NoScript** [166].

Les modules complémentaires suivants sont documentés à la section **5.0 D'autres modules utiles de Mozilla** [167] :

- **Form Fox**
- **McAfee Site Advisor**
- **Petname Tool**
- **FireGPG**

Comment régler les paramètres de sécurité et de confidentialité

Firefox comporte plusieurs options faciles à régler pour protéger votre vie privée et la sécurité de votre système chaque

fois que vous accédez à Internet. La configuration appropriée dépend de votre situation :

- Si vous êtes dans un lieu public ou au travail, vous devrez peut-être reconfigurer ces paramètres en fonction de vos besoins;
- Si vous utilisez votre ordinateur personnel et ne permettez à personne de l'utiliser pour naviguer sur Internet, vous n'aurez qu'à configurer ces paramètres une seule fois;
- Vous pouvez également transporter avec vous une version portable de Firefox sur une clé USB. Cela vous permet de configurer Firefox selon vos besoins et d'utiliser cette version personnalisée sur n'importe quel ordinateur public.

Première étape. **Sélectionnez : Outils > Options** dans le menu principal de Firefox pour activer la fenêtre *Options* :

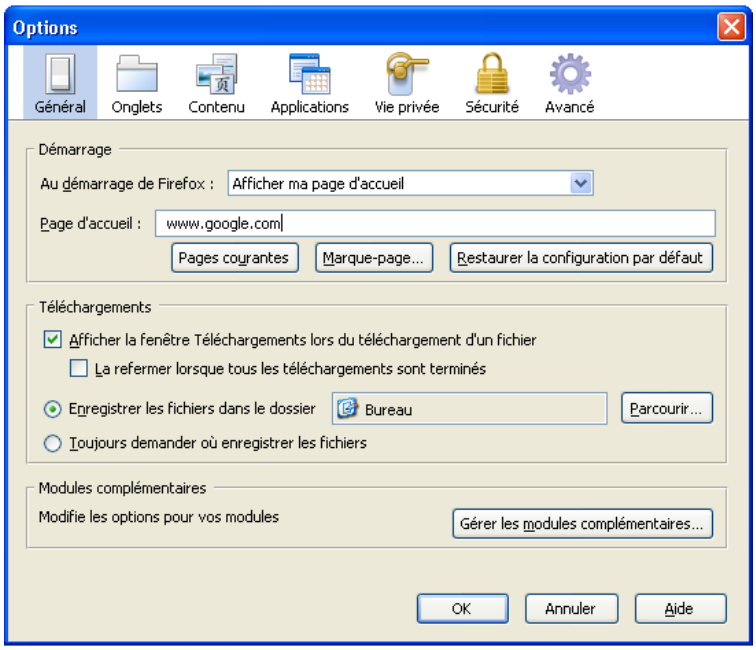


Figure 1 : La fenêtre Options, en mode Général

Commentaire : **Cliquez** sur l'onglet *Général* si la fenêtre *Général*, illustrée à la *Figure 1*, ne s'affiche pas automatiquement.

C'est ici que se trouvent les paramètres principaux de Firefox.

2.1 Comment configurer la fenêtre Vie privée

La fenêtre *Vie privée* vous permet de régler les options liées à la confidentialité et la sécurité du navigateur.

Première étape. **Cliquez** sur *Vie privée* pour activer la fenêtre ci-dessous :

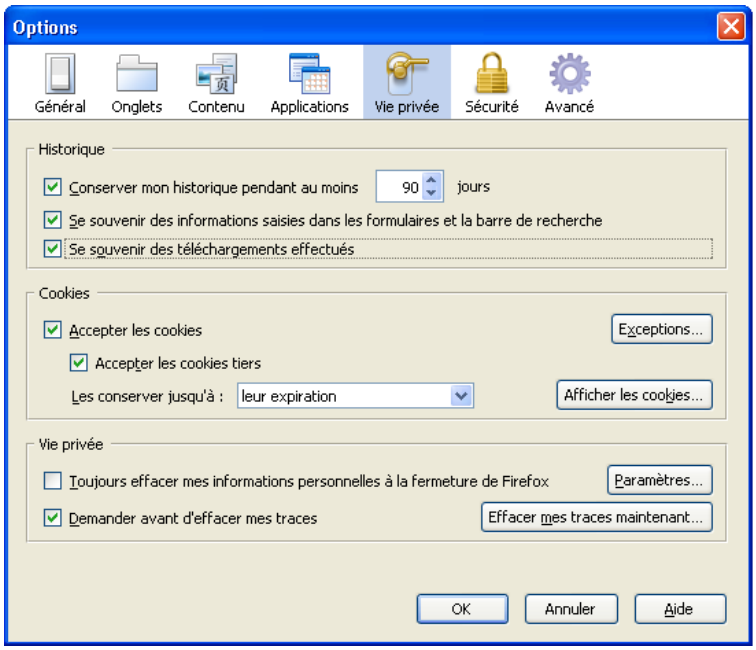


Figure 2 : La fenêtre Vie privée

- **La rubrique Historique**

Sous la rubrique *Historique*, vous pouvez gérer l'historique du navigateur Firefox, c.-à-d. la liste de tous les sites Internet que vous avez visités depuis que vous avez commencé à utiliser le programme. En désactivant les fonctions suivantes, vous ne laisserez aucune trace des adresses Internet que vous avez visitées à partir de cet ordinateur.

Deuxième étape. **Cochez** les cases appropriées pour désactiver les options *Se souvenir des pages visitées lors des [nombre] derniers jours* et *Se souvenir des informations saisies dans les formulaires et la barre de recherche* (si bien sûr ces options n'étaient pas déjà désactivées) :

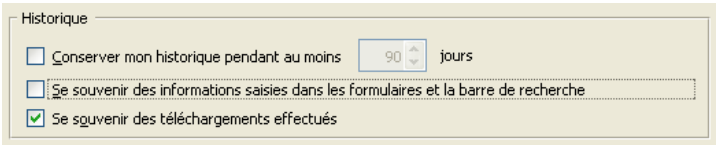

Historique
Conserver mon historique pendant au moins
90
jours
Se souvenir des informations saisies dans les formulaires et la barre de recherche
Se souvenir des téléchargements effectués

Figure 3 : Les options désactivées sous la rubrique Historique

- **La rubrique Cookies**

Sous la rubrique *Cookies*, vous pouvez déterminer si vous permettez le téléchargement des cookies sur votre ordinateur, ainsi que la "durée de vie" de ces cookies. Un cookie est un fichier utilisé pour authentifier, entretenir ou contrôler vos comportements et vos habitudes de navigation sur Internet. Chaque fois que vous visitez un site Internet particulier, les cookies associés à ce site sont automatiquement téléchargés sur votre ordinateur. Par exemple, lorsque vous ouvrez certaines pages de connexion à un service de courrier électronique, votre nom d'utilisateur apparaît automatiquement. C'est parce que ce site à placé un cookie sur votre ordinateur et y a associé votre page de connexion. Bien que plusieurs cookies soient nécessaires pour accéder à certains sites Internet et y naviguer librement, d'autres cookies sont conçus avec des intentions malveillantes. C'est pourquoi il est fortement recommandé d'effacer tous les cookies téléchargés sur votre ordinateur après chaque utilisation de Firefox. Pour plus de renseignements à ce sujet, veuillez consulter la rubrique **Vie privé e**, ci-dessous.

Troisième étape. **Activez** le menu défilant *Les conserver jusqu'à :* pour afficher les options illustrées ci-dessous :

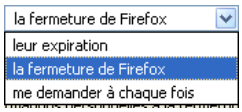


Figure 4 : Les options du menu défilant Les conserver jusqu'à :

Quatrième étape. **Sélectionnez** l'option *la fermeture de Firefox*.

- **La rubrique Vie privée**

Sous la rubrique *Vie privée*, vous pouvez déterminer comment est traitée l'information colligée lorsque vous naviguez sur Internet. Cela inclut la mémoire cache, les cookies, l'historique de navigation et les fichiers temporaires. Il est fortement conseillé d'effacer *toutes les informations personnelles* lorsque vous avez fini de naviguer sur Internet, particulièrement si vous utilisez des ordinateurs destinés à un usage public.

Cinquième étape. **Cochez** les cases appropriées pour activer les options *Toujours effacer mes informations personnelles à la fermeture de Firefox* et *Demander avant d'effacer mes traces* (si bien sûr ces options n'étaient pas déjà activées).

Sixième étape. **Cliquez** sur : et **cochez** toutes les options présentées.

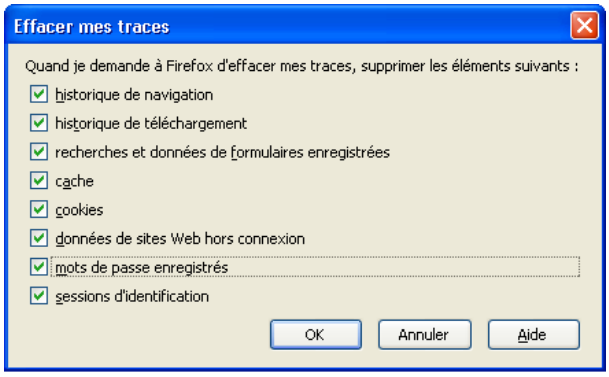
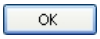
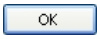


Figure 5 : L'écran Effacer mes traces

Septième étape. **Cliquez** sur :  et de nouveau sur  pour confirmer vos réglages.

Commentaire : Pour effacer vos informations personnelles conservées par le navigateur Firefox, vous pouvez en tout temps **Sélectionner : Outils > Effacer mes traces** ou **appuyer** sur les touches **Ctrl+Shift+Del**.

Les options de la rubrique *Vie privée* sont désormais réglées de telle sorte que les cookies seront effacés après chaque séance de navigation, ce qui concorde avec le comportement déjà réglé sous la rubrique 'Cookies'. Il est utile d'activer les deux options, étant donnée l'importance de supprimer les cookies. Puisque les autres renseignements personnels, tels que l'historique et les mots de passe enregistrés, ne sont visibles que par les personnes qui utilisent votre ordinateur, vous pouvez aussi choisir de ne pas tout effacer. Rappelez-vous que les cookies peuvent être envoyés aux sites Internet que vous visitez, ce qui les rend particulièrement vulnérable.

Pour des moyens avancés et sûrs de supprimer des données temporaires, veuillez consulter le . [168]

2.2 Comment configurer la fenêtre Sécurité

Entre autres choses, la fenêtre *Sécurité* vous permet de régler comment vos renseignements de connexion et vos mots de passe sont stockés. Même si la plupart des navigateurs sont pourvus d'options permettant de sauvegarder et stocker ces

renseignements, il est fortement recommandé de *ne pas* utiliser ces options, puisqu'elles comportent un risque de sécurité. Pour plus d'information sur le stockage des mots de passe, veuillez consulter le Guide pratique KeePass?.

Première étape. **Cliquez** sur *Sécurité* pour activer la fenêtre illustrée ci-dessous :

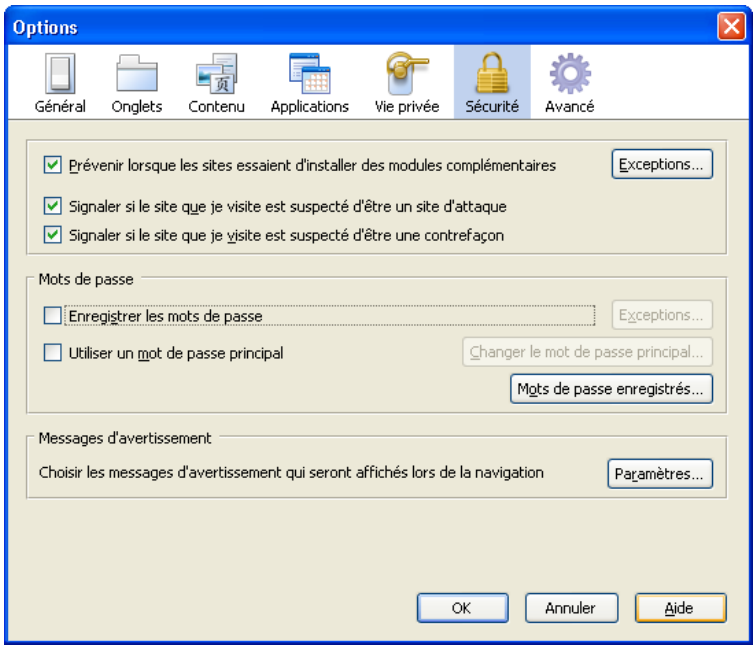


Figure 6 : La fenêtre Sécurité

Dans la première rubrique, il est conseillé d'activer l'option *Me signaler si le site que je visite est suspecté d'être une contrefaçon*. Vous pouvez aussi, en plus d'activer cette option, utiliser une combinaison de modules complémentaires détaillés à la section 5.0 D'autres modules utiles de Mozilla [167], tel que **FormFox** et **McAfee Site Advisor**, pour être automatiquement avisé lorsque vous visitez un site Internet jugé peu sûr.

Vous pouvez laisser les valeurs par défaut des autres réglages de la fenêtre *Sécurité*.

Installer des modules complémentaires Firefox

Le téléchargement et l'installation des **modules complémentaires Mozilla** est rapide et facile. Pour télécharger et installer différents modules complémentaires, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez : Démarrer > Mozilla Firefox** ou **double-cliquez** sur l'icône de bureau **Firefox** pour lancer Firefox.

Deuxième étape. **Saisissez** https://addons.mozilla.org/fr/firefox/ [169] dans la barre d'adresse, puis faites *Enter* pour ouvrir la page des modules complémentaires pour Firefox.

Troisième étape. **Saisissez** le nom du module voulu (par exemple, **NoScript**) dans la zone de recherche, puis **cliquez** sur *Search* pour trouver ce module.

Quatrième étape. **Cliquez** sur le bouton

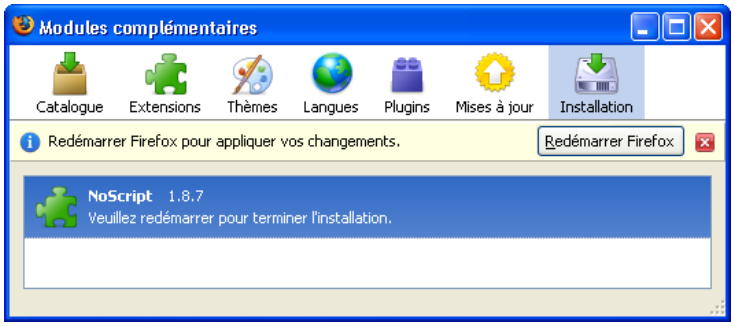
pour activer la fenêtre *Installation d'un logiciel*.

Cinquième étape. **Cliquez** sur le bouton *Installer maintenant* pour entamer l'installation.

Commentaire : Si vous installez des modules complémentaires à partir de sites qui ne font pas partie du domaine Mozilla, il est possible que vous deviez *Autoriser* ces sites à charger les fenêtre d'installation. Vous trouverez le bouton

dans le coin supérieur droit de votre navigateur.

Sixième étape. **Cliquez** sur le bouton *Redémarrez Firefox*. Firefox redémarrera avec le module complémentaire en opération.



Conseil : Vous pouvez aussi trouver quelques un de ces modules complémentaires sur d'autres sites. Il sont toujours assortis de l'extension de fichier *.xpi* (par exemple, noscript-1.6.8-fx+mz+sm.xpi).

Pour confirmer que votre module complémentaire a bien été téléchargé, **Sélectionnez : Outils > Modules**

complémentaires, dans le menu principal de Firefox, pour activer l'écran illustré ci-dessous :

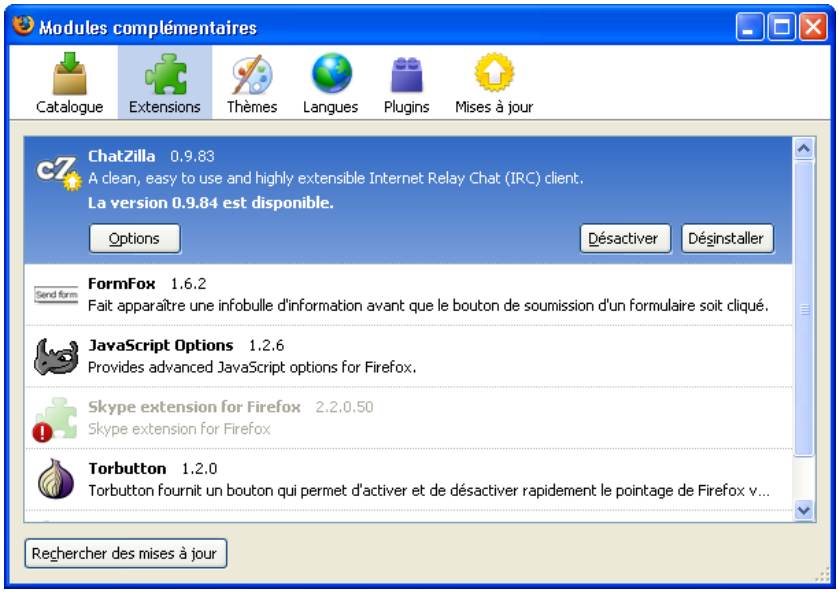

Modules complémentaires
Catalogue
Extensions
Thèmes
Langues
Plugins
Mises à jour
ChatZilla 0.9.83
A clean, easy to use and highly extensible Internet Relay Chat (IRC) client.
La version 0.9.84 est disponible.
Options
Désactiver
Désinstaller
FormFox 1.6.2
Fait apparaître une infobulle d'information avant que le bouton de soumission d'un formulaire soit cliqué.
JavaScript Options 1.2.6
Provides advanced JavaScript options for Firefox.
Skype extension for Firefox 2.2.0.50
Skype extension for Firefox
Torbutton 1.2.0
Torbutton fournit un bouton qui permet d'activer et de désactiver rapidement le pointage de Firefox v...
Rechercher des mises à jour

Figure 7 : La fenêtre Modules complémentaires de Mozilla Firefox

Commentaire : Certains modules complémentaires, notamment **McAfee SiteAdvisor**, devraient être téléchargés à partir de leur site respectif.

NoScript

NoScript est un **module complémentaire Mozilla** particulièrement utile. Ce programme peut contribuer à protéger votre ordinateur contre des sites Internet malveillants. Il fonctionne en dressant une "liste blanche" des sites que vous avez désignés comme acceptables, sûrs ou fiables (tel qu'un site de "télébanque" à domicile ou un journal électronique). Tous les autres sites sont considérés comme potentiellement dangereux et leurs fonctions sont limitées jusqu'à ce que vous décidiez que le contenu du site ne comporte aucun risque et que vous l'ajoutiez à la liste blanche.

4.1 Comment utiliser NoScript

Après avoir téléchargé NoScript et redémarré Firefox, l'icône NoScript apparaît dans le coin inférieur droit de la barre d'état de Firefox, tel qu'illustré ci-dessous :

Figure 8 : Le bouton NoScript

Commentaire : Vous vous rendrez compte qu'après avoir installé NoScript, certains sites Web ne s'afficheront plus correctement; l'explication de ce phénomène est données plus loin dans ce guide.

Pour commencer à utiliser NoScript, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur : pour activer le menu défilant illustré ci-dessous :

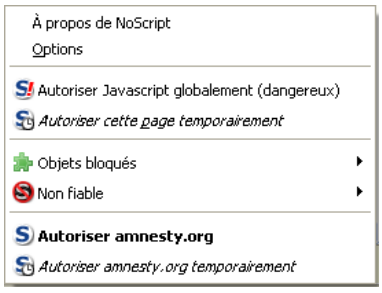


Figure 9 : Le menu défilant NoScript

NoScript comporte par ailleurs sa propre barre d'état. Le programme y affiche de l'information sur les éléments (par exemple, la publicité et les fenêtres intempestives) et les scripts dont l'exécution est actuellement bloquée par le programme. Le bouton *Options*, qui apparaît dans le coin droit, vous permet d'afficher la fenêtre *Options de NoScript*, illustrée ci-dessous :

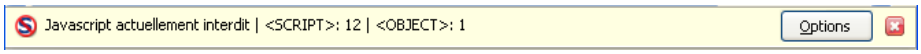


Figure 10 : La barre d'état deNoScript

Après l'installation, NoScript commencera à bloquer automatiquement toutes les publicités intempestives (*pop-up*), les bannières électroniques, le code Java et JavaScript, ainsi que tout attribut potentiellement dangereux provenant d'un site Internet. NoScript ne fait pas lui-même la différence entre un contenu dangereux et un contenu nécessaire à l'affichage normal d'un site Internet. Il vous appartient de définir des exceptions pour les sites dont vous jugez les contenus sûrs.

Voici deux exemples de NoScript à l'œuvre : à la *Figure 11*, NoScript a réussi à bloquer une publicité sur un site commercial. À la *Figure 12*, le site Internet d'**Air Canada** vous avise que JavaScript doit être activé (au moins temporairement) pour que le site s'affiche correctement.

Figure 11 : Un exemple où NoScript bloque une publicité intempestive lors d'une visite sur un site commercial

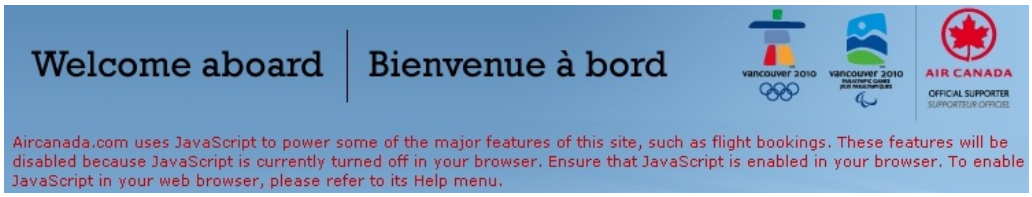

Welcome aboard
Bienvenue à bord
vancouver 2010
vancouver 2010
AIR CANADA
OFFICIAL SUPPORTER
Aircanada.com uses JavaScript to power some of the major features of this site, such as flight bookings. These features will be disabled because JavaScript is currently turned off in your browser. Ensure that JavaScript is enabled in your browser. To enable JavaScript in your web browser, please refer to its Help menu.

Figure 12 : Le site Web d'Air Canada nécessite l'activation de JavaScript

Parfois, NoScript ne bloque que partiellement JavaScript. Lorsque cela se produit, le message suivant s'affiche :

PuisqueNoScript ne fait pas la différence entre code malveillant et code légitime, il est possible que certaines fonctions et fonctionnalités importantes (par exemple, une barre d'outil) soient désactivées. Dans ce cas, vous n'avez qu'à passer à l'étape suivante :

Deuxième étape : **Cliquez** sur

et sélectionnez l'une ou l'autre des options suivantes :

- l'option *Autoriser [nom du site Internet] temporairement* pour autoriser tous les éléments de code lors de cette séances;
- l'option *Autoriser [nom du site Internet]* pour définir une règle permanente autorisant tous les éléments de code de ce site Web.

Conseil : Bien que l'utilisation de NoScript puisse paraître laborieuse au début, (parce que, par exemple, les sites Web que vous avez l'habitude de visiter ne s'affichent pas correctement), vous tirerez immédiatement avantage de la fonction de blocage automatique des éléments suspects. Cela bloquera toutes les publicités et fenêtres intempestives, ainsi que les éléments de code malveillants intégrés (ou piratés) à certains sites Web.

4.2 Comment utiliser les options de NoScript (Strictement pour utilisateurs expérimentés et avancés)

NoScript peut être configuré pour défendre votre système contre les attaques XSS (ou *Cross-site Scripting*), y compris le blocage des ressources distantes de type JAR. Un script *cross-site* est un type de faille de sécurité informatique qui permet à des pirates et autres intrus d'*injecter* un virus ou un bogue informatique dans un code existant utilisé par un navigateur Internet (en particulier les codes HTML, Java et JavaScript, ou tout autre langage de programmation supporté par un navigateur). En fait, un site Internet peut s'exposer à de nombreuses attaques depuis plusieurs sites différents si ces derniers comportent des éléments publicitaires ou des liens pointant vers ce site. De telles attaques peuvent également être générées par un site Web tiers. Si vous vous y connaissez en matière d'informatique et de logiciels, NoScript comporte plusieurs onglets permettant de configurer divers paramètres de sécurité afin de protéger vos systèmes contre ce type d'attaques.

Pour accéder à ces fonctions, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez** sur : pour activer le menu défilant du programme, puis **sélectionnez** *Options* pour afficher la fenêtre *Options de NoScript*. **Cliquez** ensuite sur l'onglet *Avancé*, illustré ci-dessous :

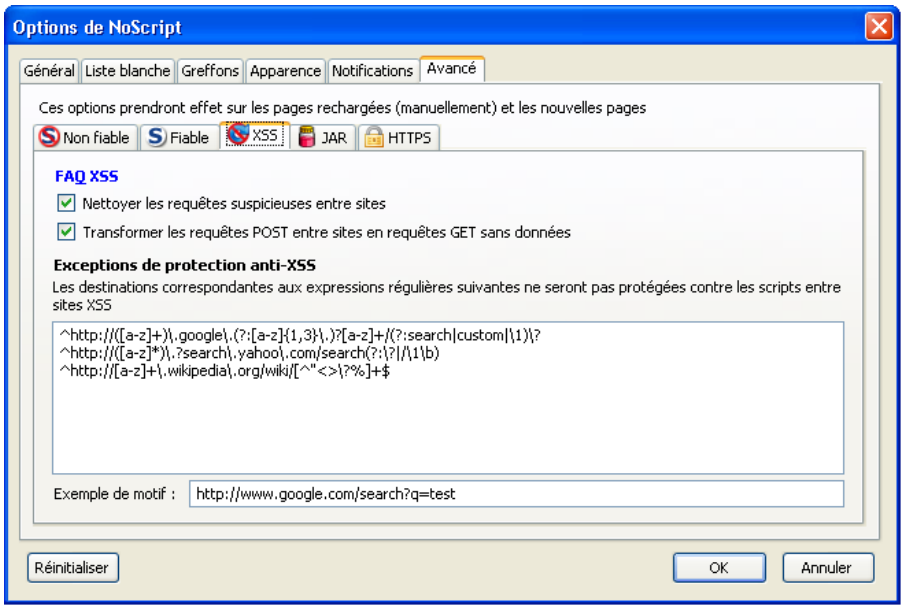


Figure 13 : La fenêtre Options de NoScript, affichant les options de l'onglet Avancé

Deuxième étape. **Cliquez** sur un onglet (par exemple *JAR* ou *XSS*), puis cochez les options appropriées et/ou définissez des exceptions, si nécessaire.

Conseil : Pour des informations détaillées à propos de NoScript, veuillez visiter http://noscript.net/ [170] et http://noscript.net/faq [171].

L'onglet *Greffons* vous laisse définir des restrictions supplémentaires pour les *sites fiables et les sites non fiables*.

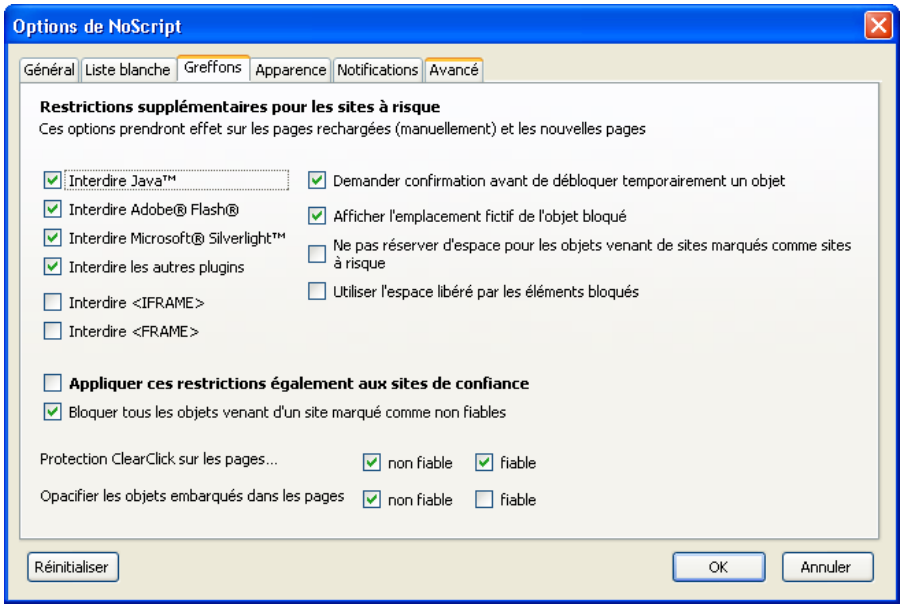

Options de NoScript
Général
Liste blanche
Greffons
Apparence
Notifications
Avancé
Restrictions supplémentaires pour les sites à risque
Ces options prendront effet sur les pages rechargées (manuellement) et les nouvelles pages
Interdire Java™
Interdire Adobe® Flash®
Interdire Microsoft® Silverlight™
Interdire les autres plugins
Interdire <IFRAME>
Interdire <FRAME>
Demander confirmation avant de débloquer temporairement un objet
Afficher l'emplacement fictif de l'objet bloqué
Ne pas réserver d'espace pour les objets venant de sites marqués comme sites à risque
Utiliser l'espace libéré par les éléments bloqués
Appliquer ces restrictions également aux sites de confiance
Bloquer tous les objets venant d'un site marqué comme non fiables
Protection ClearClick sur les pages...
non fiable
fiable
Opacifier les objets embarqués dans les pages
non fiable
fiable
Réinitialiser
OK
Annuler

Figure 14 : La fenêtre Options de NoScript affichant les options de l'onglet Greffons

D'autres modules utiles de Mozilla

Dans cette section, nous présenterons d'autres **modules complémentaires Mozilla**, tous très utiles à leur façon. Ces modules peuvent améliorer ou perfectionner la sécurité de votre système lorsque vous visitez certains sites Web et lorsque vous effectuez des transactions par Internet. Certains de ces modules fonctionnent en arrière-plan lorsque vous naviguez sur Internet.

Important : Des conflits peuvent parfois survenir entre différents outils ou différentes versions de ces outils. Si vous croyez qu'un outil a un effet négatif sur la performance générale de votre système, désinstallez-le et vérifiez si votre ordinateur fonctionne alors correctement. Si les modules complémentaires recommandés ci-dessous entrent en conflit les uns avec les autres (ce qui pourrait arriver avec NoScript, par exemple), il vous faudra décider lequel de ces modules est le plus important pour vous, et désinstaller l'autre.

Commentaire : Plusieurs sites de téléchargement exécutent des programmes JavaScript non malveillants. Si vous avez déjà installé NoScript, vous pouvez temporairement autoriser l'exécution de scripts permettant le téléchargement d'un module en particulier.

5.1 FormFox

FormFox affiche la destination réelle d'un formulaire en ligne. Le programme vous laisse déterminer s'il est sûr ou pas de soumettre des renseignements personnels tels que votre dossier de crédit, adresse de courriel, mot de passe, nom

d'utilisateur et autres renseignements. FormFox trouve et affiche la vraie destination d'un formulaire Web qui, *en apparence*, peut sembler légitime, sûr ou fiable. Avant de cliquer sur les boutons *Enter*, *Login* ou *Soumettre* dans n'importe quel formulaire électronique, glisser votre curseur au dessus du bouton pour activer une *infobulle* qui affiche la réelle destination du formulaire.

Important : Rappelez-vous que même si un formulaire est affiché dans un site sécurisé, cela ne signifie pas nécessairement que l'information soumise via le formulaire sera envoyée à une destination également sécurisée.

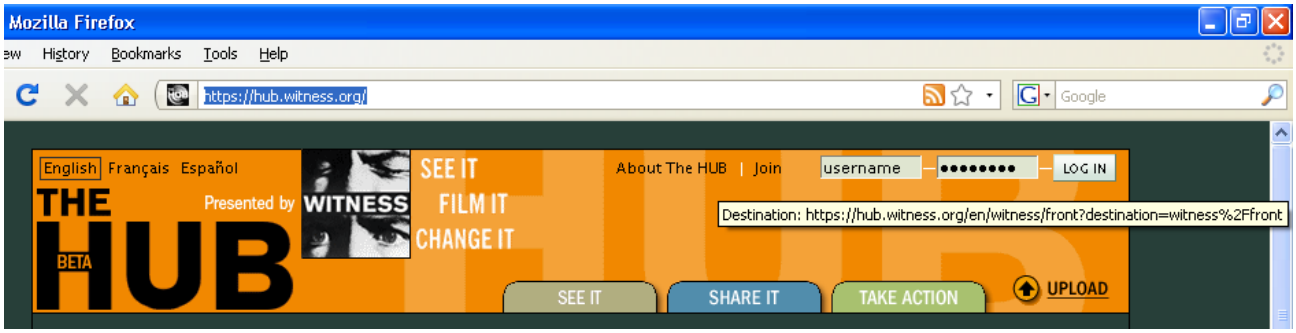


Figure 15 : Un exemple d'infobulle de FormFox

5.2 McAfee SiteAdvisor

McAfee SiteAdvisor est un logiciel propriétaire conçu pour fonctionner avec tous les navigateurs, y compris Firefox. McAfee SiteAdvisor entretient une énorme base de données en ligne contenant des renseignements sur différents sites Internet. Il affiche des renseignements sur les sites malveillants ou inconnus, ainsi que sur les sites jugés sûrs ou fiables. Il affiche par ailleurs une évaluation de la sécurité des différents liens trouvés lorsque vous effectuez une recherche sur Internet. SiteAdvisor balaie constamment Internet avec un moteur de recherche automatique pour vous aider à examiner ces sites.

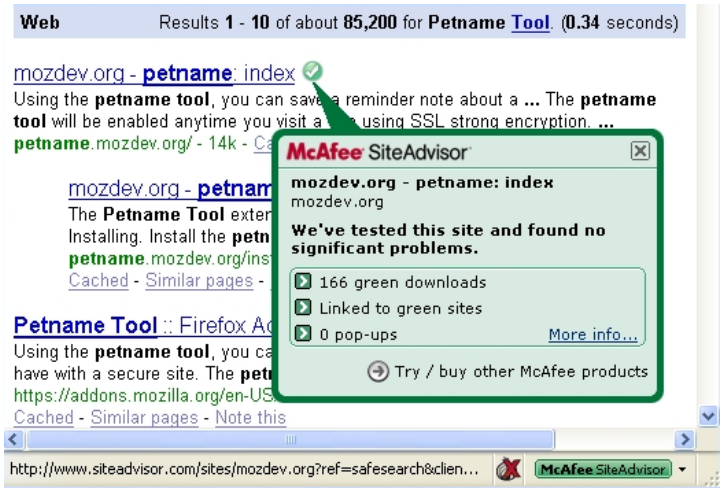

Web
Results 1 - 10 of about 85,200 for Petname Tool. (0.34 seconds)
mozdev.org - petname: index
Using the petname tool, you can save a reminder note about a ... The petname tool will be enabled anytime you visit a using SSL strong encryption. ...
petname.mozdev.org/ - 14k -
mozdev.org - petnam
The Petname Tool exter
Installing. Install the petn
petname.mozdev.org/ins
Cached - Similar pages -
Petname Tool :: Firefox A
Using the petname tool, you ca
have with a secure site. The petu
https://addons.mozilla.org/en-US
Cached - Similar pages - Note this
McAfee SiteAdvisor
mozdev.org - petname: index
mozdev.org
We've tested this site and found no significant problems.
166 green downloads
Linked to green sites
0 pop-ups
More info...
Try / buy other McAfee products
http://www.siteadvisor.com/sites/mozdev.org?ref=safesearch&clien...
McAfee SiteAdvisor

Figure 16 : Un example d'évalution d'un site par McAfee SiteAdvisor

5.3 Petname Tool

Petname Tool est un outil conçu pour vous rafraîchir la mémoire concernant votre expérience ou votre historique de navigation par rapport à un site Internet donné. Cependant, Petname Tool n'est actif que lorsque vous visitez un site utilisant le protocole **Secure Socket Layer** (**SSL** – Pour plus de renseignements à ce sujet, voir le chapitre 7. Préserver la confidentialité de vos communications sur Internet [127] du livret pratique). Une zone de texte apparaitra à droite de la barre d'outil Firefox. Vous n'avez qu'à y saisir un commentaire descriptif au sujet du site; ce commentaire apparaîtra à votre prochaine visite de ce site, vous assurant ainsi que vous visitez bel et bien le même site qu'auparavant. Cela diminue considérablement les risques de fraude par Internet, d'hameçonnage (ou *phishing*) et d'usurpation d'adresse IP. Petname s'affiche en trois modes distincts :

- Hors service, la zone de texte est grise et affiche le mot "*untrusted*" : cela indique que la page visitée n'emploie pas le protocole SSL!
- Sur un fond jaune, la zone de texte affiche le mot "*untrusted*" : cela indique que la page visitée emploie le protocole SSL.
- Sur un fond vert, la zone de texte affiche le commentaire que vous avez saisi lors d'une visite antérieure : cela indique que cette page provient d'un site SSL que vous avez déjà visité.

5.4 FireGPG

FireGPG est un module complémentaire de Firefox qui vous permet de chiffrer et déchiffrer le texte affiché sur une page Web donnée. Cette fonction est très utile pour accroître le niveau de confidentialité de vos communications par messagerie webmail. FireGPG utilise le modèle de chiffrement **Public Key Encryption (PKE)**. Ce module comporte en outre une fonction spéciale pour les comptes de courriel Gmail, qui facile davantage le processus de chiffrement.

Commentaire : FireGPG requiert l'installation préalable du logiciel de chiffrement Gnu Privacy Guard et la création d'une paire de clés.

Pour plus d'inofrmation sur le fonctionnement de SafeHistory, veuillez vous référer à http://getfiregpg.org/install.html [172]

5.5 Désinstaller des modules complémentaires de Mozilla

Pour désinstaller l'un ou l'autre des modules complémentaires, vous n'avez qu'à suivre les étapes énumérées ci-dessous :

Première étape : Dans le menu de Firefox, **sélectionnez : Outils > Modules complémentaires**

Deuxième étape : **Sélectionnez** le module voulu et **cliquez** sur *Désinstaller*

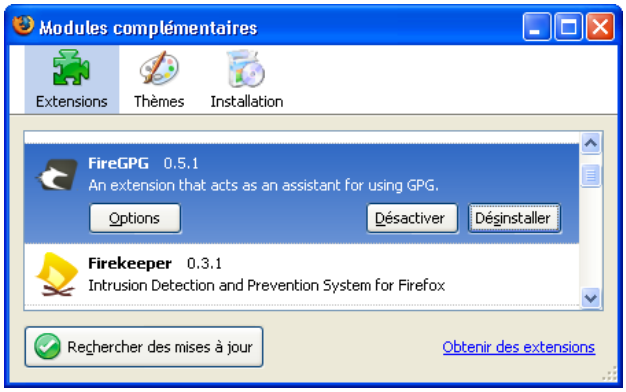


Figure 17 : La fenêtre Modules complémentaires de Firefox

Faq et questions récapitulatives

Muhindo et Salima comprennent bien les fonctions de certains **modules complémentaires pour Firefox**, mais sont un peu rebutés par d'autres. Heureusement, Assani est capable de les aider à mieux comprendre ces modules plus complexes mais tout de même fort utiles.

Q. : *Pourquoi dois-je utiliser autant de modules différents pour me défendre contre les sites Internet malveillants? Si NoScript me protège contre les scripts dangereux, par exemple, pourquoi ai-je besoin que McAfee Site Advisor m'indique quels sites sont malveillants?*

R. : *Il est souvent judicieux d'utiliser plus d'un outil pour se prémunir contre une même menace. (Les logiciels antivirus sont une exception notable à cette règle, puisqu'ils entrent habituellement en conflit les uns avec les autres.) Ces modules complémentaires de Firefox emploient des techniques différentes pour protéger ton navigateur contre une multitude de menaces. NoScript, par exemple, bloquent tous les scripts des sites Internet inconnus, mais la plupart des internautes ont tendance à approuver les sites qu'ils visitent régulièrement, ce qui ouvre automatiquement la porte à des scripts potentiellement malveillants. Les utilisateurs de NoScript ont aussi tendance à permettre aux sites inconnus de charger leurs scripts, de façon temporaire, si ces scripts sont nécessaires pour que le site s'affiche et fonctionne normalement. D'autres modules sécuritaires, comme McAfee Site Advisor, peuvent vous aider à maintenir une protection efficace dans des situations comme celles-là.*

6.1 Questions récapitulatives

1. Comment peut-on effacer l'historique de navigation, les cookies et la mémoire cache du navigateur?
2. Contre quels types d'attaques le module NoScript peut-il protéger votre système?

Tor - anonymat et contournement

Tor est un logiciel conçu pour accroître le degré d'anonymat de vos activités sur Internet. Il agit en camouflant votre identité et en brouillant la trace de vos activités sur Internet, afin que les technologies de surveillance soient incapables de vous retracer.

Site Internet

https://www.torproject.org [173]

Configuration requise :

- Compatible avec toutes les versions de Windows
- Une connexion Internet
- Maximisé pour Mozilla Firefox

Versions utilisées pour rédiger ce guide :

- Tor : 0.2.0.32
- Vidalia : 0.1.7
- TorButton : 1.2.0

Pour installer Tor

- *Lisez la courte introduction des Guides pratiques [13]*
- ***Cliquez sur l'icône ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

Tor:

[174]

Licence :

- Gratuiciel (Freeware)

Lecture préalable :

- Livret pratique Security in-a-box, chapitre 8. Préserver son anonymat et contourner la censure sur Internet [175].

Niveau : 1 : Débutant, 2 : Moyen, **3 : Intermédiaire** et **4 : Expérimenté**, 5 : Avancé

Temps d'apprentissage : 20 - 30 minutes

Ce que vous apportera l'utilisation de cet outil :

- La capacité de cacher votre identité numérique sur Internet.
- La capacité de déjouer vos fournisseurs de service Internet et les mécanismes nationaux de surveillance en dissimulant vos destinations en ligne.
- La capacité de contourner la censure et les règles de filtrage sur Internet.

1.1 À propos de cet outil

Tor est un logiciel conçu pour accroître le degré d'anonymat de vos activités sur Internet. Il agit en camouflant votre identité et en brouillant la trace de vos activités sur Internet, afin que les technologies de surveillance soient incapables de vous retracer. Que l'anonymat soit important ou pas pour vous, Tor peut s'avérer un moyen utile et sécuritaire de contourner les mesures de censure sur Internet lorsque vous naviguez (ou publiez) sur certains sites ou carnets.

Tor protège votre anonymat en routant vos communications à travers un réseau décentralisé de serveurs/relais géré par des bénévoles un peu partout dans le monde. Cela empêche d'éventuels agents espions ou malveillants de surveiller votre connexion Internet pour savoir quels sites vous avez visités et/ou pour déterminer votre position géographique (où vous vous trouvez, sur quel ordinateur vous travaillez, etc.). Quant aux bénévoles de Tor, certains d'entre eux sont en mesure de savoir que vous utilisez le logiciel, et certains autres peuvent savoir que « quelqu'un » est en train d'accéder au site que vous visitez, mais personne ne peut détenir ces deux informations en même temps.

Tor peut camoufler vos tentatives de connexion à un site en particulier, mais n'a pas été conçu pour cacher le contenu de vos communications. En conséquence, Tor peut ajouter une couche supplémentaire de protection lorsque vous l'utilisez en combinaison avec d'autres services sécurisés comme Riseup ou Gmail, mais vous ne devriez pas utiliser ce programme pour accéder à des fournisseurs de service de courrier électronique non sécurisé, comme Hotmail ou Yahoo, ou tout autre site qui accepte vos mots de passe avec une connexion 'http' non sécurisée.

Le programme Tor est livré avec la suite Vitalia. Après l'installation, vous trouverez quatre nouveaux programmes sur votre ordinateur :

- **Tor** – le programme lui-même, qui vous permet d'utiliser le réseau de connexion anonyme Tor;
- **Vidalia** – une interface graphique (GUI) pour Tor;
- **Privoxy** – un programme de proxy qui accroît votre capacité à accéder à Internet via Tor;
- **Torbutton** – un module complémentaire pour le navigateur Firefox qui vous permet d'activer et désactiver Tor facilement.

Après l'installation, Tor, Privoxy et Vidalia seront immédiatement lancés au démarrage de l'ordinateur. Les trois programmes doivent être fonctionnels pour que Tor puisse être utilisé normalement et efficacement.

Définitions :

- **Port** : Dans ce guide, le terme « port » désigne un point d'entrée à travers lequel un logiciel peut communiquer avec des services se trouvant sur d'autres ordinateurs mis en réseau. Si une URL, comme www.google.com [176], vous fournit « l'adresse » d'un service, le port vous indique quelle « porte » utiliser lorsque vous arrivez à la bonne destination. Lorsque vous naviguez sur Internet, vous utilisez habituellement le port 80 pour les sites non sécurisés (http://mail.google.com [177]) et le port 443 pour les sites sécurisés (https://mail.google.com [178]).
- **Proxy** : Dans ce guide, le terme « proxy » désigne un logiciel intermédiaire – sur votre ordinateur, votre réseau local ou quelque part d'autre sur Internet – qui contribue à relayer votre communication jusqu'à sa destination finale.
- **Route** : Dans ce guide, le terme « route » désigne le chemin de communication sur Internet entre votre ordinateur et le serveur de destination.
- **Relais passerelle** : Un relais passerelle (ou passerelle) est un serveur Tor qui facilite votre première entrée dans le réseau de connexion anonyme Tor. Les passerelles sont optionnelles et sont conçues pour être utilisées dans les pays où l'accès à Tor est bloqué.

Comment accéder au réseau Tor

Après avoir installé la suite Vidalia, vous remarquerez de nouveaux icônes sur votre *Bureau* et dans le menu **Démarrer**. La **Barre des tâches** Windows (dans le coin inférieur droit de votre écran) affiche maintenant l'icône *Privoxy* et l'icône *Vidalia* .

L'icône Vidalia change d'apparence pour indiquer si Tor est en fonction ou non. Vous n'avez qu'à **cliquer à droite** pour *Arrêter Tor* ou *Lancer Tor*.

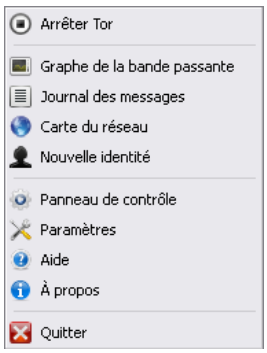


Figure 1 : Le menu Vidalia de la barre des tâches

Lorsque vous arrêtez le service Tor, l'icône apparaît ainsi :

Vous pouvez également lancer **Privoxy** et **Vidalia** depuis le menu *Démarrer* en suivant les étapes énumérées ci-dessous :

Première étape. **Sélectionnez : Démarrer > Programmes > Vidalia Bundle > Privoxy > Privoxy**

Deuxième étape. **Sélectionnez : Démarrer > Programmes > Vidalia Bundle > Vidalia**

Avant de continuer, assurez-vous que Privoxy et Vidalia sont activés et apparaissent dans la barre des tâches.

2.1 Le panneau de contrôle de Vidalia

Le *Panneau de contrôle de Vidalia* présente une interface graphique pour les nombreuses fonctionnalités de Tor.

Figure 2 : Le Panneau de contrôle de Vidalia

Lorsque vous ouvrez le panneau de contrôle, le programme tente automatiquement de se connecter au réseau Tor. Une barre de progression vous indique l'état de la connexion.

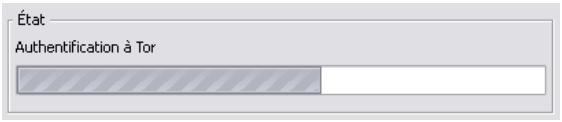


Figure 3 : L'état lors du démarrage de Tor

Commentaire : Avant de se connecter au réseau, Tor doit accomplir un série de tâches. La première tentative risque d'être considérablement plus longue que les connexions futures. C'est parce que Tor prend un certain temps pour se familiariser avec le réseau et ses fonctions, et télécharge ensuite les renseignements nécessaires sur votre ordinateur.

Si la tentative de connexion est réussie, l'écran suivant s'affichera :

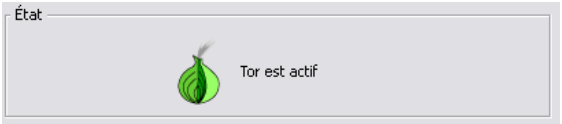


Figure 4 : La rubrique d'État de Tor – Tor est actif

Si, pour une raison ou une autre, la connexion ne s'établit pas, veuillez consulter la **Section 4 : Résolution des problèmes sous Tor** [179].

2.2 Comment naviguer sur Internet en utilisant Tor

La prochaine étape, avant de commencer à naviguer sur Internet via Tor, est de configurer votre navigateur Internet. Veuillez lire attentivement l'une des sections suivantes, selon le navigateur que vous utilisez avec Tor. Nous recommandons fortement l'utilisation du navigateur Mozilla Firefox [180].

2.2.1 Consignes pour Mozilla Firefox

Première étape. **Lancez** Firefox.

Après l'installation de la suite Vidalia, un nouveau bouton s'affiche dans le coin inférieur droit du navigateur.

Le module complémentaire **Torbutton** est l'outil que vous utiliserez dorénavant pour déterminer si votre navigateur doit accéder à Internet via le réseau Tor ou via une connexion Internet normale. À l'installation initiale, Torbutton est éteint et l'étiquette affiche *Tor inactif*.

Deuxième étape. **Cliquez** sur le Torbutton. Le bouton prend maintenant cet aspect :

Votre navigateur est maintenant configuré pour accéder aux pages Internet de façon anonyme via le réseau Tor.

Conseil : Lorsque vous avez fini de naviguer, assurez-vous de supprimer tous vos fichiers Internet temporaires et vos cookies, et de vider votre mémoire cache. Cela peut être facilement accompli en **sélectionnant : Outils > Effacer mes traces**, en **cochant** toutes les options disponibles et en **cliquant** sur le bouton *Effacer mes traces maintenant*. Pour plus de renseignements, veuillez consulter le Guide pratique Mozilla Firefox [180].

2.2.2 Consignes pour Internet Explorer

Commentaire : Même s'il est possible d'utiliser Tor avec n'importe quel navigateur Internet, vous devriez éviter d'utiliser Internet Explorer si l'anonymat est un facteur important pour vous. Il est beaucoup plus difficile à une tierce partie de découvrir votre identité si vous utilisez Firefox avec le module complémentaire Torbutton.

Première étape. **Lancez** le navigateur Internet Explorer.

Deuxième étape. **Sélectionnez : Outils > Options Internet** pour afficher la fenêtre *Options Internet*.

Troisième étape. **Cliquez** sur l'onglet *Connexions* pour afficher la fenêtre illustrée ci-dessous :

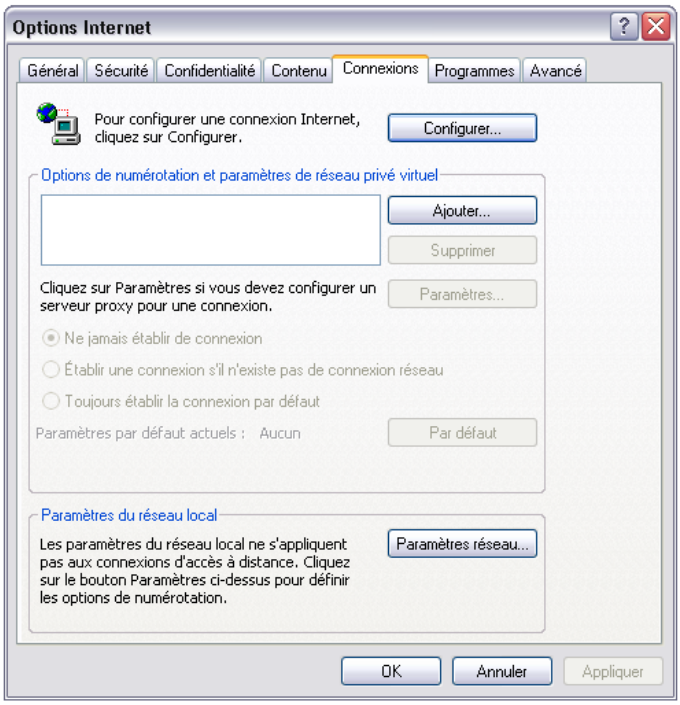

Options Internet
Général
Sécurité
Confidentialité
Contenu
Connexions
Programmes
Avancé
Pour configurer une connexion Internet, cliquez sur Configurer.
Configurer...
Options de numérotation et paramètres de réseau privé virtuel
Ajouter...
Supprimer
Cliquez sur Paramètres si vous devez configurer un serveur proxy pour une connexion.
Paramètres...
Ne jamais établir de connexion
Établir une connexion s'il n'existe pas de connexion réseau
Toujours établir la connexion par défaut
Paramètres par défaut actuels : Aucun
Par défaut
Paramètres du réseau local
Les paramètres du réseau local ne s'appliquent pas aux connexions d'accès à distance. Cliquez sur le bouton Paramètres ci-dessus pour définir les options de numérotation.
Paramètres réseau...
OK
Annuler
Appliquer

Figure 5 : L'onglet Connexions de la fenêtre Options Internet

Quatrième étape. **Cliquez** sur le bouton *Paramètres réseau…* pour afficher la fenêtre *Paramètres du réseau local*, illustrée ci-dessous :

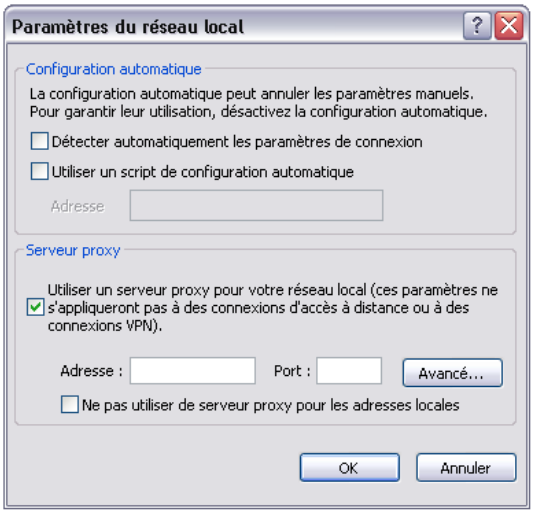

Paramètres du réseau local
Configuration automatique
La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.
Détecter automatiquement les paramètres de connexion
Utiliser un script de configuration automatique
Adresse
Serveur proxy
Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliqueront pas à des connexions d'accès à distance ou à des connexions VPN).
Adresse :
Port :
Avancé...
Ne pas utiliser de serveur proxy pour les adresses locales
OK
Annuler

Figure 6 : Paramètres du réseau local

Cinquième étape. **Cochez** la case *Utiliser un serveur proxy…* et **cliquez** sur le bouton *Avancé* pour activer la fenêtre *Paramètres du proxy* .

Sixième étape. **Remplissez** les champs vide pour régler les paramètres du proxy, tel qu'indiqué ci-dessous :

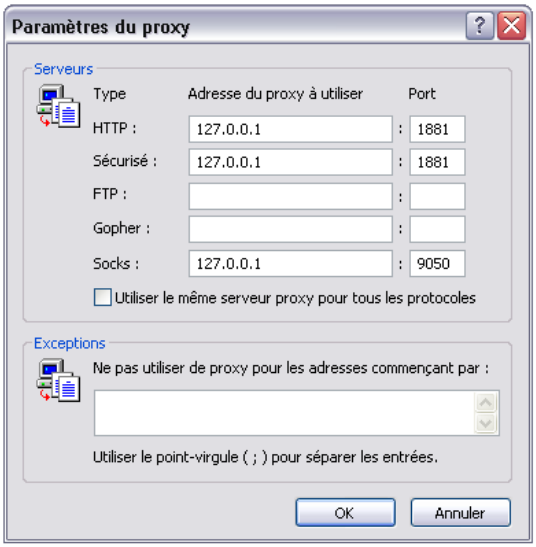


Figure 7 : Les paramètres du proxy dans Internet Explorer

Septième étape. **Cliquez** sur le bouton *OK* trois fois de suite, ou jusqu'à ce que vous soyez de retour à la fenêtre principale du navigateur.

Commentaire : Vous devrez répéter les **étapes 1 à 4** pour interrompre le service Tor. À **l'étape 5**, vous devrez plutôt **décocher** l'option *Utiliser un serveur proxy….*

Conseil : Lorsque vous avez terminé votre séance de navigation, n'oubliez pas de supprimer votre mémoire cache de fichiers Internet temporaires et vos cookies. Vous pouvez effectuer cette opération en **sélectionnant : Outils > Options Internet** puis en **cliquant** sur *Supprimer les cookies*, puis *OK*; en **cliquant** sur *Supprimer les fichiers*, puis *OK*; en **cliquant** sur *Effacer l'historique*, puis *Oui*; et finalement en cliquant sur *OK*.

2.3 Comment vérifier votre connexion à Tor

Première étape. **Ouvrez** le site Internet https://check.torproject.org/ [181]. Le site vous confirmera si vous êtes connecté ou non au réseau Tor.

Figure 8 : La fenêtre 'Are you using Tor?' de Mozilla Firefox

Félicitations! Votre navigateur Web est connecté à Internet via le réseau Tor. Les sites Internet qui sont habituellement bloqués dans votre pays vous seront désormais accessibles, et vos destinations en ligne resteront cachées pour toute personne tentant de surveiller votre connexion Internet. Vous remarquerez aussi que certains sites Internet, tel que Google [www.google.com], tiendra parfois pour acquis que vous vous trouvez dans un pays différent. Cela est normal lorsque vous utilisez Tor.

S'il y a un problème avec votre connexion Tor, vous verrez peut-être apparaître cette fenêtre :

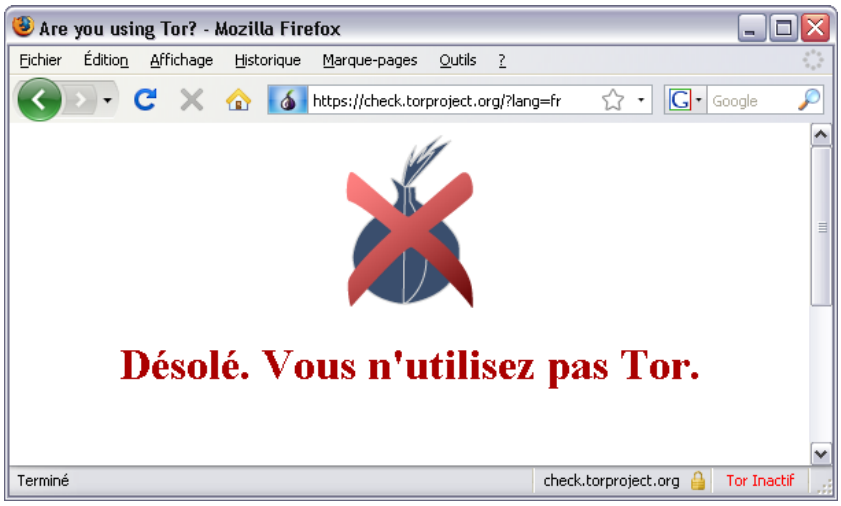


Figure 9 : La fenêtre Vous n'utilisez pas Tor

Si vous voyez apparaître ce message, ou si la page que vous cherchez ne s'affiche pas normalement, veuillez consulter la section **4.0 Résolution des problèmes sous Tor** [179].

Avertissement : Si vous utilisez un module complémentaire de Firefox offrant un service de proxy (comme FoxyProxy), vous devriez le désactiver avant d'activer Torbutton, sinon, Tor risque de ne pas fonctionner normalement.

À propos du Panneau de contrôle de Vidalia

L'interface graphique est accessible par le *Panneau de contrôle de Vidalia* (*Figure 2*), que vous avez déjà utilisé pour lancer Tor. Les autres fonctions du panneau de contrôle sont explorées ci-dessous.

Double-cliquez sur : pour lancer le *Panneau de contrôle de Vidalia*.

3.1 Pour visualiser la connexion au réseau Tor

Cliquez sur :

Figure 10 : La carte du réseau Tor

La carte du réseau Tor affiche l'ensemble des serveurs Tor disponible dans la liste de *Relais* du panneau de gauche. La liste *Connexion*, dans le panneau qui se trouve sous la carte, affiche les noms des serveurs Tor choisis au hasard comme relais de

votre connexion anonyme. Si vous cliquez sur l'une ou l'autre des rangées de cette liste, le trajet emprunté par votre connexion Tor sera affiché sur la carte.

Commentaire : Cette information est présentée uniquement pour démontrer comment Tor fonctionne. Vous n'avez pas à vous inquiéter de comprendre tous les éléments de cette fenêtre.

3.2 Pour visualiser et régler les paramètres de Tor et Vidalia

Cliquez sur :

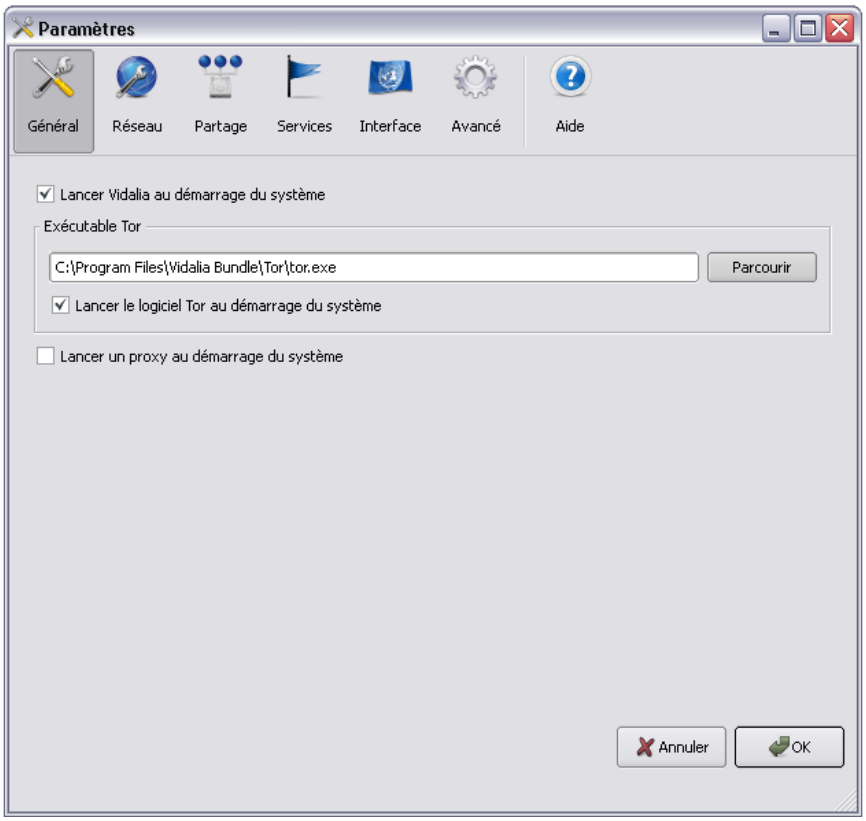


Figure 11: La fenêtre Paramètres du Panneau de contrôle de Vidalia

Sous l'onglet *Général*, vous pouvez préciser si Vidalia doit être lancé automatiquement au démarrage de Windows, et si Tor devrait être également lancé à ce moment. Vous pouvez laisser les deux options cochées, tel qu'illustré ci-dessus à la *Figure 11*.

Sous l'onglet *Interface*, vous pouvez sélectionner la langue de l'interface de Vidalia. Les autres options de cette rubrique sont décrites dans les sections suivantes du guide.

3.3 Pour interrompre le service Tor

Cliquez sur :

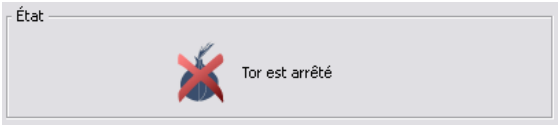


Figure 12 : La rubrique d'État de Tor – Tor est arrêté

Résolution des problèmes sous Tor

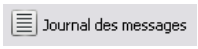
Il y a plusieurs facteurs qui peuvent faire en sorte que Tor ne fonctionne pas normalement. Certains des problèmes les plus communs sont décrits ci-dessous, avec des suggestions de solutions. Avant de continuer, assurez-vous que les quatre programmes inclus dans la suite Vidalia sont installés et fonctionnent normalement. Toutes les fonctions décrites dans cette section sont accessibles par le *Panneau de contrôle de Vidalia*.

Commentaire : Une des meilleurs façons de s'assurer que programme nouvellement installé sous Windows fonctionne correctement est de redémarrer le système. Une proportion remarquablement élevée d'erreurs courantes peuvent être réglées de cette manière!

4.1 Comment afficher le Journal des messages

En tout temps, lorsque Tor est en fonction, même lorsque le programme tente d'établir une connexion initiale, vous pouvez accéder au journal des messages. Cela peut vous aider à déterminer si le logiciel fonctionne et, ci ça n'est pas le cas, de

trouver les causes du ou des problèmes.

Cliquez sur : 

Le *Journal des messages* qui s'affiche alors devrait ressembler à la *Figure 13*, ci-dessous :

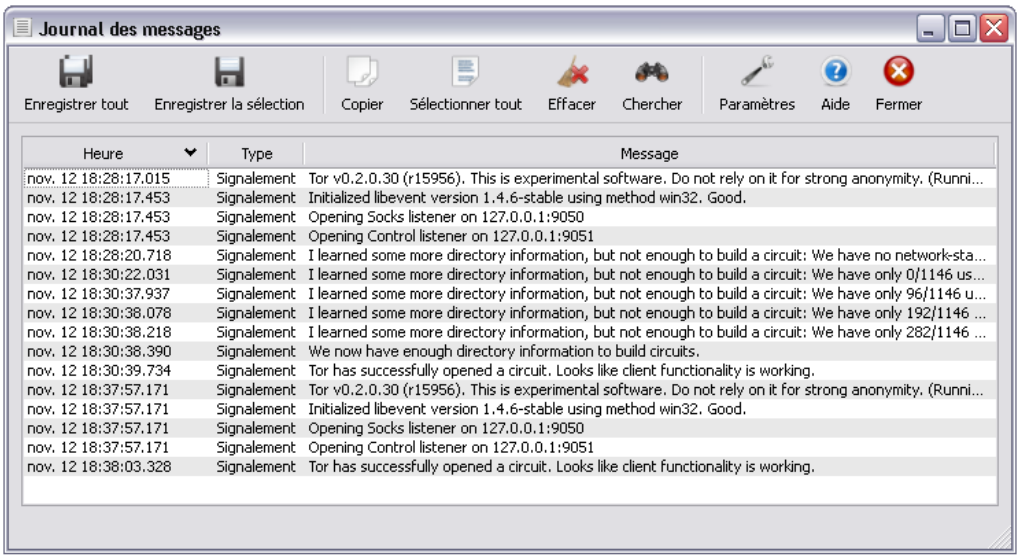

Journal des messages
Enregistrer tout
Enregistrer la sélection
Copier
Sélectionner tout
Effacer
Chercher
Paramètres
Aide
Fermer
Heure
Type
Message
nov. 12 18:28:17.015 Signalement Tor v0.2.0.30 (r15956). This is experimental software. Do not rely on it for strong anonymity. (Runni...
nov. 12 18:28:17.453 Signalement Initialized libevent version 1.4.6-stable using method win32. Good.
nov. 12 18:28:17.453 Signalement Opening Socks listener on 127.0.0.1:9050
nov. 12 18:28:17.453 Signalement Opening Control listener on 127.0.0.1:9051
nov. 12 18:28:20.718 Signalement I learned some more directory information, but not enough to build a circuit: We have no network-sta...
nov. 12 18:30:22.031 Signalement I learned some more directory information, but not enough to build a circuit: We have only 0/1146 us...
nov. 12 18:30:37.937 Signalement I learned some more directory information, but not enough to build a circuit: We have only 96/1146 u...
nov. 12 18:30:38.078 Signalement I learned some more directory information, but not enough to build a circuit: We have only 192/1146 ...
nov. 12 18:30:38.218 Signalement I learned some more directory information, but not enough to build a circuit: We have only 282/1146 ...
nov. 12 18:30:38.390 Signalement We now have enough directory information to build circuits.
nov. 12 18:30:39.734 Signalement Tor has successfully opened a circuit. Looks like client functionality is working.
nov. 12 18:37:57.171 Signalement Tor v0.2.0.30 (r15956). This is experimental software. Do not rely on it for strong anonymity. (Runni...
nov. 12 18:37:57.171 Signalement Initialized libevent version 1.4.6-stable using method win32. Good.
nov. 12 18:37:57.171 Signalement Opening Socks listener on 127.0.0.1:9050
nov. 12 18:37:57.171 Signalement Opening Control listener on 127.0.0.1:9051
nov. 12 18:38:03.328 Signalement Tor has successfully opened a circuit. Looks like client functionality is working.

Figure 13 : Le journal des messages de Vidalia

Ce journal montre que Tor a été lancé et continuera à afficher des messages portant sur le fonctionnement de Tor. Ne vous inquiétez pas trop du signalement concernant le "experimental software". Malgré ce qui est indiqué ici, Tor est l'outil de connexion anonyme le mieux éprouvé à ce jour. Il existe cependant quelques messages d'erreur que vous devriez chercher si vous éprouvez des difficultés avec le programme:

- *connection_create_listener(): Could not bind to 127.0.0.1:9050: Address already in use. Is Tor already running?*

Ce message signifie qu'un autre processus Tor a déjà été entamé. La solution la plus simple dans ce cas est de fermer Vidalia et de redémarrer votre ordinateur.

- *Vidalia was unable to start Tor. Check your settings to ensure the correct name and location of your Tor executable is specified*

Cette erreur ce produit lorsque Vidalia est incapable de trouver le fichier exécutable de Tor, *tor.exe*. Effectuez une recherche de ce fichier sur votre ordinateur et précisez son emplacement sous l'onglet *Général* de la fenêtre *Paramètres* de Vidalia.

- *I have learned some directory information, but not enough to build a circuit*

Ce message peut apparaître de façon répétée lorsque Tor démarre, et peut même continuer à s'afficher par la suite si vous avez une connexion Internet particulièrement lente. Ce message signifie simplement que Tor continue à télécharger de l'information sur le réseau.

Lorsque Tor est enfin prêt à être utilisé, le journal affiche le message suivant :

- *Tor has successfully opened a circuit. Looks like client functionality is working.*

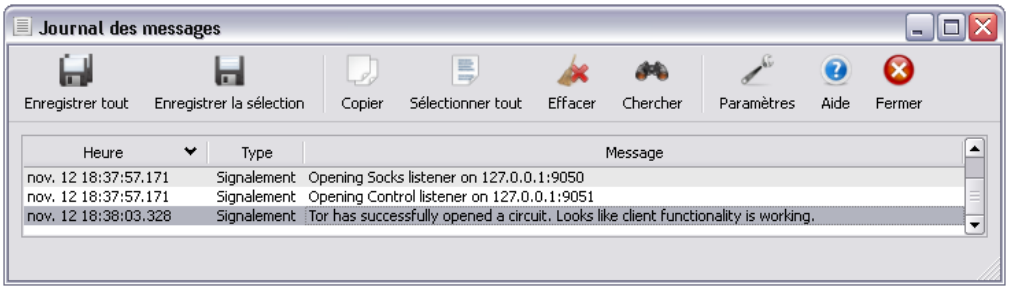


Figure 14 : Le message Tor has successfully connected (Tor a réussi à se connecter)

Ce message indique que Tor a réussi à établir une route à travers son réseau et semble fonctionner normalement. Si vous utilisez Firefox, vous devez encore activer le Torbutton avant de pouvoir naviguer sur Internet de façon anonyme. Si vous utilisez un autre navigateur, vous devez d'abord régler les paramètres du proxy pour être en mesure de vous connecter à Internet via Tor.

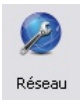
Si le journal n'affiche aucun nouveau message pendant quinze minutes, après avoir affiché le message *Opening Control listener* ou le message *Tor has learned some directory information, but not enough to build a circuit*, il vous faudra peut-être ajuster les paramètres réseau de Tor. Il est possible que votre connexion Internet actuelle exige que vous utilisiez un proxy Web particulier, ou bloque certains ports. Il est aussi possible que votre gouvernement ou votre fournisseur de service Internet ait bloqué l'accès au réseau Tor.

4.2 Les paramètres réseau de Tor

Vous devez peut-être suivre quelques étapes si vous vous rendez compte que Tor ne fonctionne plus normalement ou si le programme n'arrive pas à se connecter lorsque vous l'installez et le lancez. Essayez tout d'abord de changer les paramètres de connexion au réseau relatifs au proxy, aux ports ou aux relais, tel que décrit ci-dessous.

Première étape. **Arrêtez** le service Tor dans Vidalia.

Deuxième étape. **Ouvrez** la fenêtre des *Paramètres de Vidalia*.

Troisième étape . **Cliquez** sur : 

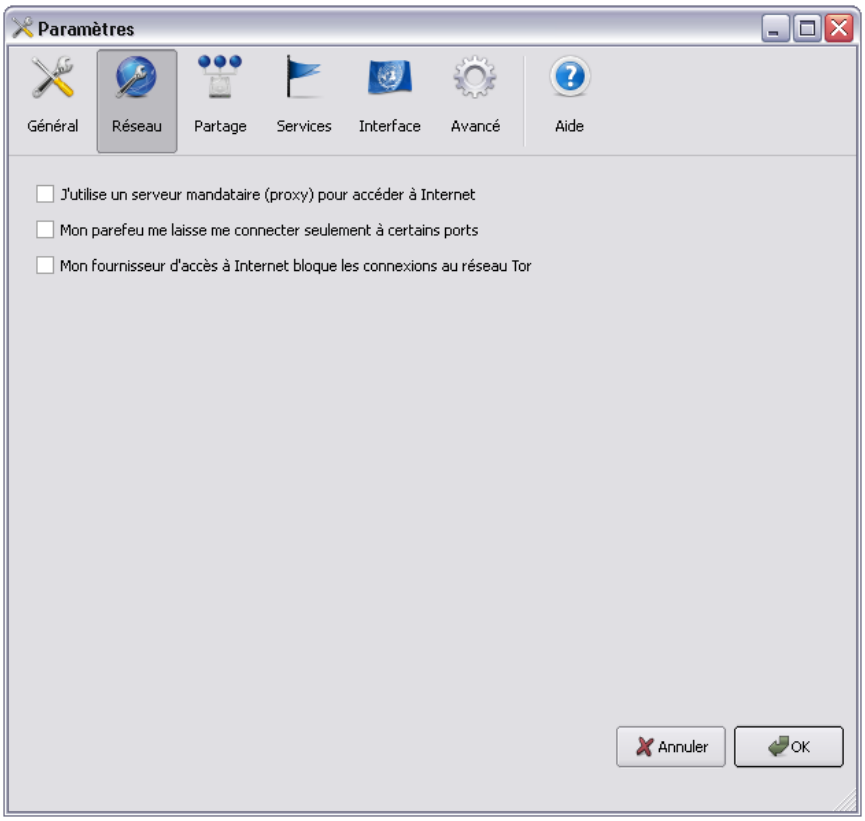


Figure 15 : La fenêtre des paramètres réseau du Panneau de contrôle de Vidalia

Lorsque vous aurez terminé de régler ces paramètres, **cliquez** sur le bouton *OK* pour fermer la fenêtre des paramètres réseau, puis **Lancez** le service Tor dans Vidalia.

4.2.1 Utiliser un serveur mandataire (proxy)

Si vous devez utiliser un serveur mandataire (ou proxy) pour accéder à Internet, alors saisissez les renseignements nécessaires dans cette fenêtre. En règle générale, cela est plutôt requis par les réseaux de sociétés privées ou universitaires, mais des proxys sont occasionnellement requis par des cafés Internet, ou même par le gouvernement pour couvrir l'accès à Internet dans certains pays. Si les renseignements de proxy nécessaires ne sont pas clairement indiqués, vous devrez peut-être vous adresser à un administrateur du réseau ou à une personne qui utilise la même connexion Internet que vous.

Première étape. **Cochez** l'option *J'utilise un serveur mandataire (proxy) pour accéder à Internet*.

Deuxième étape. **Saisissez** les renseignements du proxy dans les zones appropriées.

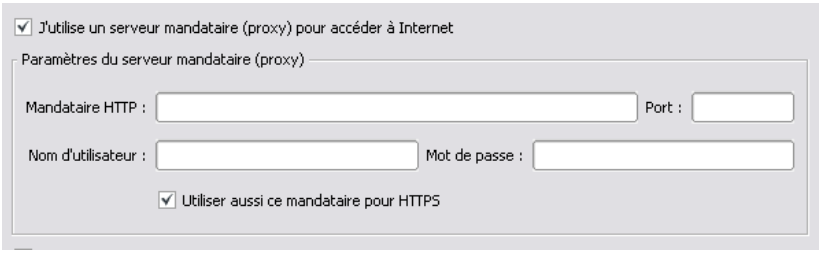

J'utilise un serveur mandataire (proxy) pour accéder à Internet
Paramètres du serveur mandataire (proxy)
Mandataire HTTP :
Port :
Nom d'utilisateur :
Mot de passe :
Utiliser aussi ce mandataire pour HTTPS

Figure 16 : La rubrique des détails du Proxy

4.2.2 Les restrictions de ports

Certains réseaux ou paramètres informatiques peuvent restreindre l'accès à certains ports. Si vous êtes en mesure de naviguer normalement sur Internet, vous pouvez compter sur au moins deux ports ouverts (80 et 443). Vous pouvez régler Tor pour fonctionner exclusivement avec ces deux ports.

Première étape. **Cochez** l'option *Mon pare-feu me laisse me connecter seulement à certains ports*.

Deuxième étape. La zone *Ports autorisés* devrait normalement afficher '80,443', tel qu'illustré ci-dessous:

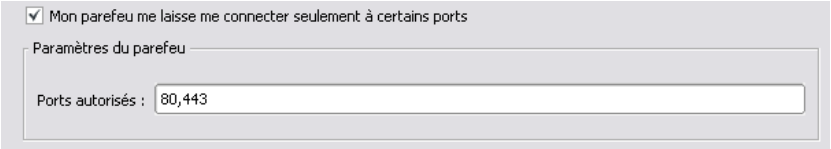


Figure 17 : La rubrique Paramètres du pare-feu spécifiant les ports ouverts sur le réseau

4.2.3 Utiliser un relais passerelle

Si vous ne pouvez toujours pas vous connecter au réseau Tor, il vous reste encore deux options :

Première option : Consultez le wiki Tor FAQ wiki [182] pour trouver des suggestions de marches à suivre.

Deuxième option : Vous résidez peut-être dans l'un des quelques pays qui bloquent l'accès à Tor depuis l'Internet national. Dans ce cas, vous devrez utilisez un relais passerelle pour accéder à Tor.

Les passerelles vous permettent d'accéder au réseau anonyme Tor, même si l'accès est bloqué de l'intérieur de votre pays, en intégrant une 'première étape' cachée dans le réseau. Pour utiliser cette fonction, vous devez indiquer l'emplacement d'au moins une passerelle. Idéalement, vous devriez saisir l'adresse de trois passerelles ou plus. Si vous connaissez une personne de confiance qui utilise déjà une passerelle, vous pouvez lui demander de partager ces renseignements avec vous. Vous pouvez aussi utiliser une des deux méthodes proposées par la Base de données de passerelles du Projet Tor. Pour commencer, vous pouvez envoyez un courriel à [bridges@torproject.org], à partir de n'importe quel compte Gmail, avec les mots "get bridges" dans le corps du message. La base de données vous acheminera alors les adresses de trois passerelles. (N'oubliez pas, vous devriez TOUJOURS vous connecter à votre compte Gmail par la page https://mail.google.com [178]!). Sinon, vous pouvez également accéder au site Internet de la Base de données de passerelles à https://bridges.torproject.org/ [183] (sans utiliser Tor), qui affiche les renseignements associés à trois passerelles différentes.

Commentaire : La Base de données de passerelles est conçue pour empêcher qui que ce soit de se renseigner facilement sur toutes les passerelles, c'est pourquoi il est possible que les mêmes passerelles s'affichent chaque fois que vous effectuez un requête en vous connectant au site. Si vous attendez suffisamment longtemps, de nouveaux renseignements s'afficheront.

Première étape. **Cochez** l'option *Mon fournisseur d'accès à Internet bloque les connexions au réseau Tor*.

Deuxième étape. **Saisissez** ou **collez** l'adresse d'un relais passerelle dans la zone *Ajouter une passerelle*. Tel qu'illustré par à la *Figure 18*, les renseignements de la passerelle comprennent une adresse IP et un numéro de port, comme *79.47.201.97:443*, et peuvent aussi inclure une longue série de chiffres et de lettres à la fin, comme par exemple *80E03BA048BFFEB4144A4359F5DF7593A8BBD47B*.

Troisième étape. **Cliquez** sur :

Quatrième étape. Recommencez les étapes précédentes pour chaque nouvelle adresse de passerelle. Il est recommandé d'en saisir au moins trois.

Mon fournisseur d'accès à Internet bloque les connexions au réseau Tor
Paramètres de Passerelle
Ajouter une passerelle :
Comment puis-je trouver un relais passerelle ?
79.47.201.97:443 80E03BA048BFFEB4144A4359F5DF7593A8BBD47B

Figure 18 : Ajouter une adresse de relais passerelle

4.3 Désinstaller la suite Vidalia

Pour désinstaller toutes les composantes de la suite Vidalia, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez : Démarrer> Programmes > Vidalia Bundle > Uninstall**

Deuxième étape. **Choisissez** une langue pour l'assistant, puis **cliquez** sur *Suivant*.

Troisième étape. **Cochez** tous les éléments de la suite alors affichés dans la fenêtre.

Désinstallation de Vidalia Bundle
Choisissez les composants
Cochez les composants de Vidalia Bundle que vous souhaitez désinstaller.
Cochez les composants que vous désirez désinstaller et décochez ceux que vous ne désirez pas désinstaller. Cliquez sur Suivant pour continuer.
Sélectionnez les composants à désinstaller :
Tor 0.2.0.30
Vidalia 0.1.7
Privoxy 3.0.6
Description
Passez le curseur de votre souris sur un composant pour en voir la description.
Espace requis : 0.0Ko
Vidalia Bundle 0.2.0.30-0.1.7 (Rev. 1)
< Précédent
Suivant >
Annuler

Quatrième étape. **Cliquez** sur *Suivant* puis sur *Désinstaller*.

Comment régler le module complémentaire Torbutton

Niveau : **4: Expérimenté**

En plus de déterminer si Firefox utilise ou non Tor pour naviguer sur Internet, le module complémentaire Torbutton accroît la sécurité et l'anonymat de votre service Tor en remédiant à certaines failles de Firefox. Sans Torbutton, un site Internet ou un serveur Tor malveillant pourrait révéler certaines informations à propos de votre emplacement sur Internet et vos activités en ligne, même lorsque vous utilisez Tor. Heureusement, Torbutton s'installe avec une configuration par défaut très sûre. Vous pouvez modifier ces paramètres vous-même, mais vous ne devriez pas le faire à moins d'avoir une assez bonne connaissance des enjeux de sécurité relatifs aux navigateurs.

La fenêtre des *préférences de Torbutton* comporte trois onglets qui vous permettent de régler trois options différentes :

- L'onglet **Paramètres du proxy**
- L'onglet **Paramètres de sécurité**
- L'onglet **Paramètres d'affichage**

Il est possible d'accéder à la fenêtre des *Préférences Torbutton*, que Torbutton soit activé ou non. Pour afficher la fenêtre des *Préférences Torbutton*, suivez les étapes énumérées ci-dessous :

Première étape. **Cliquez à droite** sur le Torbutton pour afficher le menu :

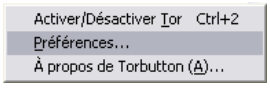


Figure 19 : Le menu de Torbutton

Deuxième étape. **Sélectionnez** l'option *Préférences...* pour afficher la fenêtre ci-dessous :

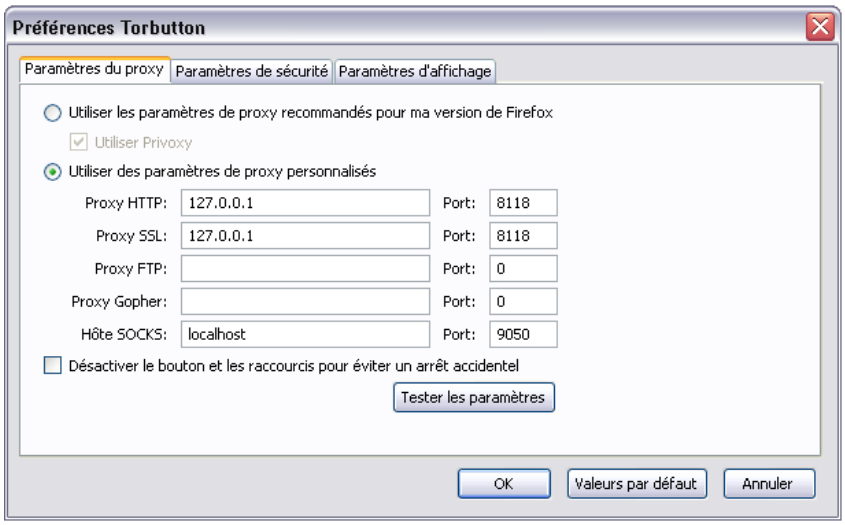

Préférences Torbutton
Paramètres du proxy
Paramètres de sécurité
Paramètres d'affichage
Utiliser les paramètres de proxy recommandés pour ma version de Firefox
Utiliser Privoxy
Utiliser des paramètres de proxy personnalisés
Proxy HTTP: 127.0.0.1 Port: 8118
Proxy SSL: 127.0.0.1 Port: 8118
Proxy FTP: Port: 0
Proxy Gopher: Port: 0
Hôte SOCKS: localhost Port: 9050
Désactiver le bouton et les raccourcis pour éviter un arrêt accidentel
Tester les paramètres
OK
Valeurs par défaut
Annuler

Figure 20 : La fenêtre des Préférences Torbutton *affichant l'onglet des paramètres du proxy*

5.1 L'onglet des Paramètres du proxy

L'onglet des *Paramètres du proxy* sert à déterminer comment Firefox accède à Internet lorsque Torbutton est actif. En temps normal, il n'est pas nécessaire de modifier ces paramètres.

5.2 L'onglet des Paramètres de sécurité

L'onglet des *Paramètres de sécurité* est conçu pour les utilisateurs ayant une connaissance avancée des navigateurs Internet et de la sécurité Internet. Les réglages par défaut assurent un niveau de sécurité élevé aux utilisateurs moyens. Cet onglet vous permet de régler comment Torbutton gère l'historique de navigation, la mémoire cache, les cookies et les autres fonctionnalités de Firefox.

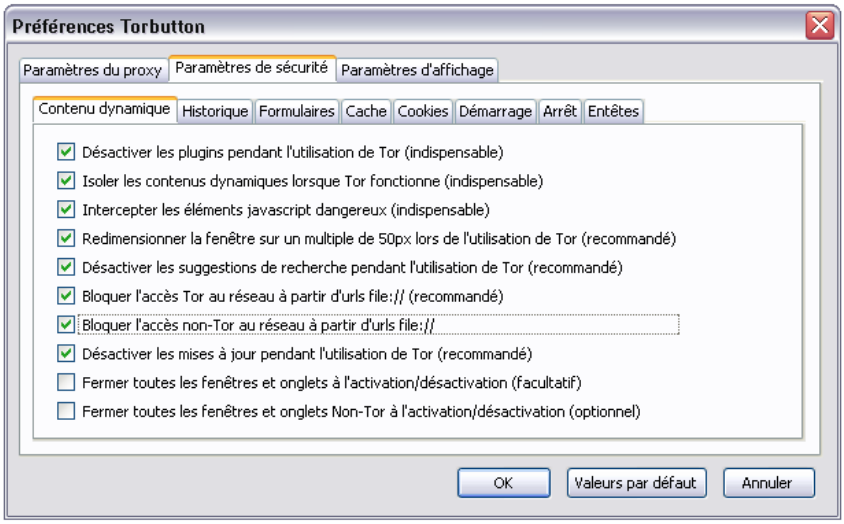

Préférences Torbutton
Paramètres du proxy
Paramètres de sécurité
Paramètres d'affichage
Contenu dynamique
Historique
Formulaires
Cache
Cookies
Démarrage
Arrêt
Entêtes
Désactiver les plugins pendant l'utilisation de Tor (indispensable)
Isoler les contenus dynamiques lorsque Tor fonctionne (indispensable)
Intercepter les éléments javascript dangereux (indispensable)
Redimensionner la fenêtre sur un multiple de 50px lors de l'utilisation de Tor (recommandé)
Désactiver les suggestions de recherche pendant l'utilisation de Tor (recommandé)
Bloquer l'accès Tor au réseau à partir d'urls file:// (recommandé)
Bloquer l'accès non-Tor au réseau à partir d'urls file://
Désactiver les mises à jour pendant l'utilisation de Tor (recommandé)
Fermer toutes les fenêtres et onglets à l'activation/désactivation (facultatif)
Fermer toutes les fenêtres et onglets Non-Tor à l'activation/désactivation (optionnel)
OK
Valeurs par défaut
Annuler

Figure 21 : L'onglet des Paramètres de sécurité

L'option *Désactiver les plugins pendant l'utilisation de Tor* est l'un des seuls paramètres de sécurité que vous devrez possiblement changer, bien que si vous le faites, cela devrait être une mesure temporaire. Afin d'afficher des contenus vidéo en ligne via Tor, plusieurs sites Internet (dont YouTube [184], DailyMotion [185] et ' The Hub [186]' de Witness) vous obligent à **décocher** cette option. Vous devriez activer les plugins uniquement lorsque vous visitez des sites de confiance, et rétablir immédiatement le paramètre par défaut lorsque vous avez fini de visiter ce site, en retournant à l'onglet des *Paramètres de sécurité* et en **cochant** cette option.

Pour plus d'information sur la fonction particulière de chaque option de l'onglet des *Paramètres de sécurité* , veuillez consulter le Site Internet de Torbutton [187].

5.3 L'onglet des Paramètres d'affichage

L'onglet des *Paramètres d'affichage* vous permet de choisir comment le Torbutton est affiché dans la barre d'état de Firefox, soit par l'icône d'oignon, soit en texte. La fonctionnalité opère de façon identique d'une manière ou d'une autre.

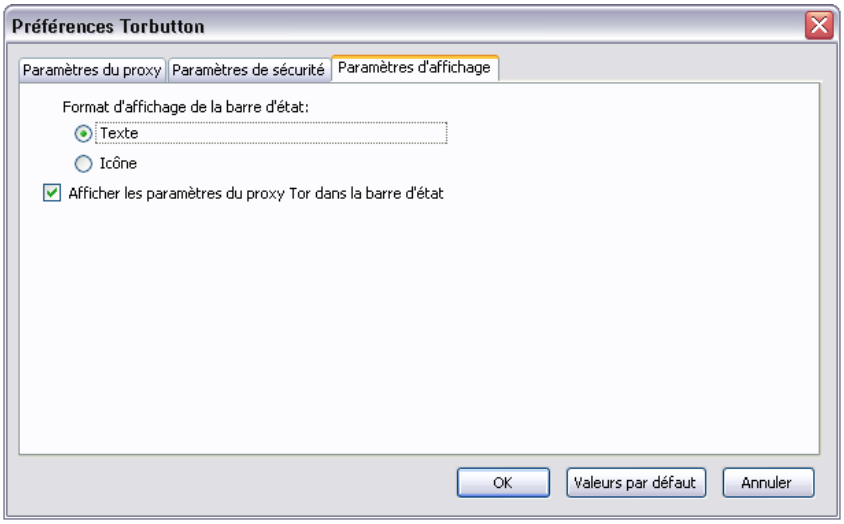


Figure 22 : L'onglet des Paramètres d'affichage

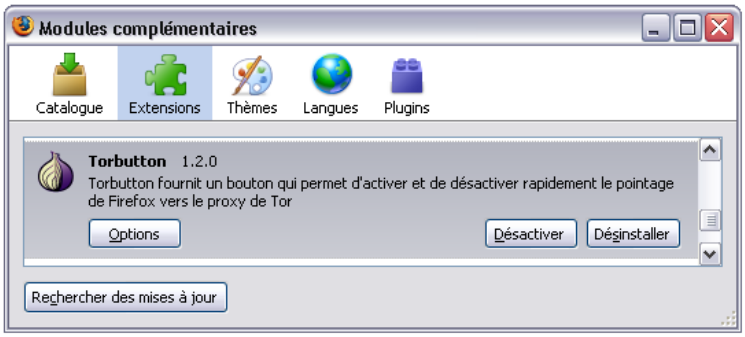
Pour plus d'information sur Torbutton, veuillez consulter la page de FAQ de Torbutton [188].

5.4 Supprimer le Torbutton

Pour supprimer le module complémentaire Torbutton de Mozilla Firefox, suivez les étapes énumérées ci-dessous :

Première étape. **Sélectionnez : Outils > Modules complémentaires**

Deuxième étape. **Sélectionnez** le module complémentaire Torbutton, puis **cliquez** sur *Désinstaller*



Troisième étape. **Redémarrez** Firefox

Le Pack de navigation Tor

Aperçu du pack de navigation Tor

Configuration requise

- Compatible avec toutes les versions de Windows

Version

- 1.1.3

Site Internet

- http://www.torproject.org/torbrowser/index.html.fr/ [189]

Licence :

* Gratuiciel (Freeware) GPL

Niveau : 1 : Débutant, **2: Moyen**, 3 : Intermédiaire et 4: Expérimenté, 5: Avancé

Temps d'apprentissage : 10 minutes

6.1 À propos de cet outil

Le **Pack de navigation Tor**, ou **Tor Browser**, est une version portable du système Tor décrit ci-dessus. Le pack comprend Tor, Vidalia, Torbutton, Firefox et **Polipo**, qui est en fait un substitut de Privoxy. Tous ces logiciels peuvent être lancés directement à partir d'une clé USB. Le Pack de navigation Tor est une solution idéale si vous voulez utiliser Tor sur un ordinateur public ou si vous ne voulez pas installer la suite Vidalia au complet sur votre ordinateur. Il est aussi très facile à utiliser.

Vous pouvez par ailleurs télécharger une version plus volumineuse du Pack de navigation Tor qui inclut le programme de messagerie instantanée Pidgin. Cette version de Pidgin est conçue et configurée pour fonctionner via Tor, et comprend le module OTR, ce qui vous permet de clavarder de façon sécurisée (chiffrée). Vous pouvez apprendre à utiliser Pidgin en consultant le chapitre 7 : Préserver la confidentialité de vos communications sur Internet et le Guide pratique Pidgin.

Commentaire : Vous devez fermer Firefox avant de lancer le Pack de navigation Tor. Si vous lisez actuellement ce guide dans un navigateur Internet, nous vous recommandons d'en imprimer une copie ou de télécharger la version PDF? avant de continuer.

6.2 Comment installer le Pack de navigation Tor

Première étape. **Téléchargez** le fichier d'installation et sauvegardez-le sur votre *Bureau*.

Deuxième étape. **Double-cliquez** sur :

pour lancer l'extraction du fichier.

Il est possible que Windows ou votre logiciel antivirus vous envoie un *Avertissement de sécurité*. **Cliquez** sur *Exécuter* ou lancez l'installation d'une manière ou d'une autre.

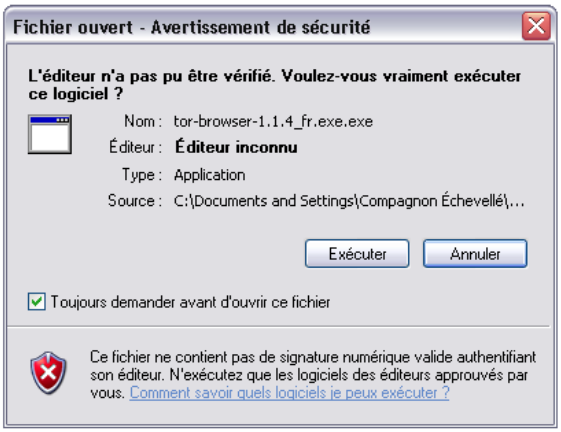

Fichier ouvert - Avertissement de sécurité
L'éditeur n'a pas pu être vérifié. Voulez-vous vraiment exécuter ce logiciel ?
Nom : tor-browser-1.1.4_fr.exe.exe
Éditeur : Éditeur inconnu
Type : Application
Source : C:\Documents and Settings\Compagnon Échevellé\...
Exécuter
Annuler
Toujours demander avant d'ouvrir ce fichier
Ce fichier ne contient pas de signature numérique valide authentifiant son éditeur. N'exécutez que les logiciels des éditeurs approuvés par vous. Comment savoir quels logiciels je peux exécuter ?

Figure 23 : L'avertissement de sécurité – Fichier ouvert

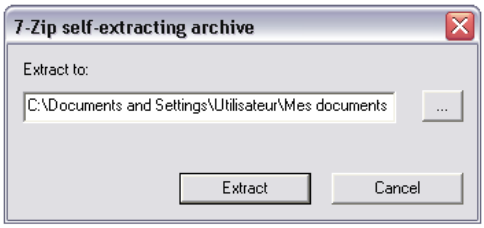


Figure 24 : La fenêtre 7-Zip self-extracting archive

Vous devrez alors indiquer un emplacement sur votre ordinateur où l'assistant d'installation procédera à l'extraction du Pack de navigation Tor. Vous pouvez aussi sélectionner une clé USB (comme le *volume amovible* illustré à la *Figure 25*) afin de créer un copie portable du Pack de navigation Tor. Sinon, vous pouvez également extraire le dossier dans n'importe quel répertoire et le déplacer à votre guise à un emplacement de votre choix.

Troisième étape. **Cliquez** sur : et **sélectionnez** le répertoire d'installation.

Figure 25 : La fenêtre Rechercher un dossier

Après l'extraction des fichiers, un nouveau répertoire appelé *Tor Browser* apparaîtra à l'emplacement choisi. Vous y trouverez l'icône de Tor Browser

.

6.3 Comment utiliser le Pack de navigation Tor

Première étape. **Double-cliquez** sur :

Le programme lancera alors Tor et l'interface graphique Vidalia, qui fonctionneront exactement tel que décrit dans les précédentes sections du guide.

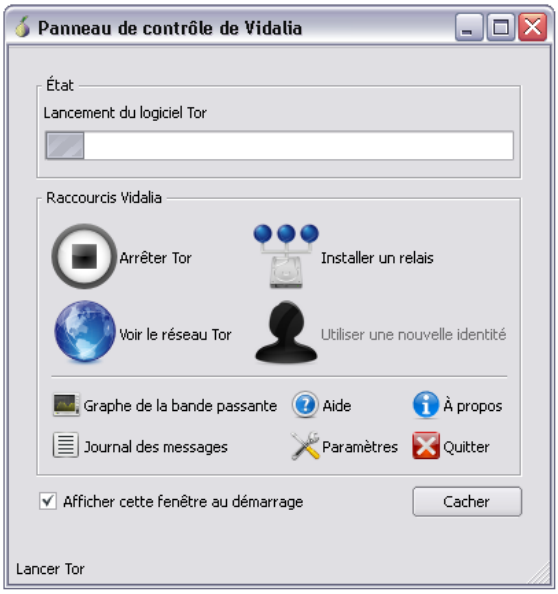


Figure 26 : La panneau de contrôle de Vidalia

Lorsque Tor a terminé le processus de démarrage, le programme lance automatiquement Firefox et vous mène directement à la page https://check.torproject.org [190], qui vous indique si vous êtes ou non connecté au réseau Tor.

Faq et questions récapitulatives

Tor est un logiciel extrêmement bien testé et entretenu. Le réseau de connexion anonyme est utilisé par des milliers de personnes, un peu partout sur la planète, et des améliorations constantes en ont fait un système de plus en plus stable et sûr. Même si certaines des explications apportées dans ce guide peuvent sembler complexes, dans la plupart des cas, vous n'aurez même pas à dépasser la section **2.0 Comment accéder au réseau Tor** [191] pour être en mesure d'utiliser le programme normalement.

Mansour a lu attentivement le chapitre 8 [175] du livret pratique, qui porte sur les mesures de contournement de la censure, et il vient tout juste de terminer la lecture du Guide pratique Tor [192]. Il lui reste cependant quelques questions pour Magda, qui, elle, utilise Tor depuis plusieurs années.

Q. : *Pourquoi devrais-je utiliser Tor?*

R. : *Bonne question. Tor est un outil fort pratique pour contourner la censure sur Internet afin d'accéder à certains sites. Ce programme est aussi très utile si l'on souhaite cacher les sites que l'on visite à notre fournisseur de service Internet, ou encore si l'on ne veut pas que les sites Internet puissent déterminer où l'on se trouve.*

Q. : *Quelle est la différence entre le Pack de navigation Tor et la version de Tor que je dois installer?*

R. : *Le Pack de navigation Tor peut être sauvegardé sur une clé USB et utilisé sur n'importe quel ordinateur, y compris le tien. Tu n'auras pas besoin de le réinstaller. Par contre, si tu installes la suite Vidalia sur ton ordinateur, Tor sera un peu plus rapide. De plus, en tenant pour acquis que tu utilisais déjà Firefox, tu auras accès à tes marque-pages existants et aux modules complémentaires déjà installés lorsque tu utiliseras Tor.*

Q. : *Il y a un message d'erreur dans le Journal des messages que je ne comprends pas. Que devrais-je faire?*

R. : *Consulte le wiki de FAQ de Tor pour voir si ton message s'y trouve. Tu peux également cliquer sur l'icône Aide dans le Panneau de contrôle de Vidalia et consulter la section 'Dysfonctionnements'.*

6.1 Questions récapitulatives

- Combien de serveurs Tor sont utilisés pour établir une connexion via le réseau Tor? Où peut-on trouver davantage d'information à propos de ces serveurs?
- Quels paramètres doivent être modifiés dans votre navigateur Internet pour que celui-ci puisse accéder à des pages Internet via Tor?
- Quels sont les programmes qui doivent être activés pour que vous soyez en mesure d'accéder au réseau Tor?
- Comment peut-on faire en sorte que l'interface Vidalia ne soit pas lancée chaque fois que Windows démarre?

URL source (Obtenu le *04/13/2011 - 14:26*): https://security.ngoinabox.org/fr/handsonguides

Liens:
[1] https://security.ngoinabox.org/fr/handsonguides
[2] http://www.avast.com/fr-fr/free-antivirus-download
[3] http://www.avast.com
[4] https://security.ngoinabox.org/fr/chapter-1
[5] http://www.free-av.com/
[6] http://free.avg.com/
[7] http://www.avast.com/en-eu/mac-edition
[8] http://www.kaspersky.co.uk/kaspersky-anti-virus-for-mac
[9] http://www.mcafee.com/us/small/products/virusscan_for_mac/virusscan_for_mac.html
[10] http://www.sophos.com/products/enterprise/endpoint/security-and-control/
[11] http://www.symantec.com/norton/products
[12] https://security.ngoinabox.org/fr/avast_virus#4.9
[13] https://security.ngoinabox.org/handsonguides
[14] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/avast/setupeng.exe
[15] http://www.imgburn.com/

[16] http://www.avg.com/us-en/avg-rescue-cd
[17] http://support.kaspersky.com/viruses/rescuedisk/
[18] http://www.f-secure.com/linux-weblog/files/f-secure-rescue-cd-release-3.00.zip
[19] http://download.bitdefender.com/rescue_cd/
[20] http://free.antivirus.com/hijackthis/
[21] http://free.antivirus.com/clean-up-tools/
[22] http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx
[23] http://technet.microsoft.com/en-us/sysinternals
[24] http://www.avast.com/download-update
[25] http://www.safer-networking.org/fr/mirrors/index.html
[26] http://www.safer-networking.org/fr
[27] https://security.ngoinabox.org/fr/avast_principale
[28] https://security.ngoinabox.org/fr/comodo_principale
[29] https://security.ngoinabox.org/fr/firefox_principale
[30] http://superantispyware.com
[31] http://www.malwarebytes.org/mbam.php
[32] http://www.microsoft.com/windows/products/winfamily/defender
[33] http://www.lavasoft.com/
[34] http://www.javacoolsoftware.com/spywareblaster.html
[35] https://security.ngoinabox.org/spybot_advance
[36] https://security.ngoinabox.org/security.ngoinabox.org/fr/ccleaner_registredewindows#4.0
[37] https://security.ngoinabox.org/fr/chapter-6
[38] http://www.safer-networking.org/fr/howto/update.hs.html
[39] http://personalfirewall.comodo.com/free-download.html
[40] http://www.personalfirewall.comodo.com
[41] http://www.netfilter.org/
[42] https://help.ubuntu.com/community/Gufw
[43] http://blog.bodhizazen.net/linux/firewall-ubuntu-gufw/
[44] http://www.hanynet.com/noobproof/
[45] http://www.lobotomo.com/products/IPSecuritas/
[46] http://www.obdev.at/products/littlesnitch/index.html
[47] http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm
[48] http://free.agnitum.com/
[49] http://www.keepass.info/download.html
[50] https://security.ngoinabox.org/fr/keepass_utiliser
[51] http://www.keepass.info/translations.html
[52] http://www.keepass.info/
[53] https://security.ngoinabox.org/fr/chapter-3
[54] http://www.keepassx.org/
[55] http://passwordsafe.sourceforge.net/
[56] http://agilewebsolutions.com/products/1Password
[57] https://security.ngoinabox.org/fr/keepass_motsdepasse
[58] https://security.ngoinabox.org/fr/keepass_portable
[59] http://security.ngoinabox.org/fr/recuva_principale
[60] http://www.truecrypt.org/downloads
[61] https://security.ngoinabox.org/fr/truecrypt_volumestandard#2.0
[62] http://www.truecrypt.org/localizations
[63] http://www.truecrypt.org/
[64] https://security.ngoinabox.org/fr/chapter-4
[65] http://www.ubuntu.com/
[66] http://www.saout.de/misc/dm-crypt/
[67] http://code.google.com/p/cryptsetup/
[68] http://sd4l.sourceforge.net/
[69] http://www.nathansheldon.com/files/
[70] http://www.ce-infosys.com/english/free_compusec/free_compusec.aspx
[71] http://www.cryptoexpert.com/lite/
[72] http://www.axantum.com/AxCrypt/
[73] https://www.steganos.com/us/products/for-free/locknote/overview/
[74] http://security.ngoinabox.org/fr/truecrypt_portable
[75] http://www.truecrypt.org/docs/
[76] https://security.ngoinabox.org/fr/truecrypt_volumescaches
[77] https://security.ngoinabox.org/fr/keepass_principale
[78] https://security.ngoinabox.org/fr/truecrypt_volumestandard#2.2
[79] http://forums.truecrypt.org/
[80] http://security.ngoinabox.org/fr/truecrypt_principale
[81] http://www.truecrypt.org/faq.php
[82] http://www.educ.umu.se/~cobian/cobianbackup.htm
[83] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/cobian/Cb7Setup.exe
[84] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/cobian/cbSetup8.exe
[85] https://security.ngoinabox.org/chapter-5
[86] https://security.ngoinabox.org/cobian_creercopie
[87] http://www.zipgenius.it/
[88] https://security.ngoinabox.org/cobian_chiffrer
[89] https://security.ngoinabox.org/truecrypt_principale
[90] https://security.ngoinabox.org/chapter-4
[91] https://security.ngoinabox.org/cobian_compresser
[92] http://www.piriform.com/recuva/builds
[93] http://www.piriform.com/recuva
[94] https://security.ngoinabox.org/fr/chapter-5
[95] http://www.r-tt.com/data_recovery_linux/
[96] http://www.cgsecurity.org/
[97] http://ntfsundelete.com/
[98] http://diskdigger.org/
[99] http://www.pcinspector.de/Default.htm?language=1
[100] http://undeleteplus.com/
[101] https://security.ngoinabox.org/fr/recuva_scan
[102] https://security.ngoinabox.org/fr/recuva_recuperer
[103] https://security.ngoinabox.org/fr/recuva_faq
[104] http://www.heidi.ie
[105] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/eraser/EraserSetup32.exe
[106] https://security.ngoinabox.org/chapter-6
[107] https://security.ngoinabox.org/undelete_principale
[108] https://security.ngoinabox.org/ccleaner_principale
[109] http://www.piriform.com/ccleaner/builds
[110] http://www.ccleaner.com
[111] http://bleachbit.sourceforge.net/
[112] http://doc.ubuntu-fr.org/nettoyer_ubuntu
[113] http://www.titanium.free.fr/
[114] https://security.ngoinabox.org/fr/ccleaner_questions
[115] https://riseup.net/
[116] https://security.ngoinabox.org/fr/chapter-7
[117] http://security.ngoinabox.org/fr/thunderbird_principale

[118] https://security.ngoinabox.org/fr/riseup_modifierparametres#4.3
[119] https://mail.riseup.net
[120] https://help.riseup.net/security
[121] https://mail.riseup.net/
[122] https://user.riseup.net/
[123] https://security.ngoinabox.org/riseup_creeruncompte#2.1
[124] http://pidgin.im
[125] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/pidginotr/pidgin-2.7.1.exe
[126] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/pidginotr/pidgin-otr-3.2.0-1.exe
[127] https://security.ngoinabox.org/chapter-7
[128] http://dashboard.aim.com/aim
[129] http://www.google.com/talk/
[130] http://www.icq.com
[131] http://www.mirc.com/
[132] http://www.msn.com/
[133] http://www.qq.com/
[134] http://chat.yahoo.com
[135] https://security.ngoinabox.org/pidgin_googletalk
[136] mailto:thierry.letesteur@gmail.com
[137] https://www.vaultletsoft.com/
[138] http://www.vaultletsoft.com/start/downloads.html
[139] mailto:terrence.letesteur@vaultletsoft.com
[140] https://security.ngoinabox.org/vaultletsuite_questions
[141] http://www.mozillamessaging.com/fr/thunderbird/
[142] http://enigmail.mozdev.org/download/index.php
[143] http://www.gnupg.org/download/index.en.html#auto-ref-2
[144] http://www.mozilla.com/thunderbird/
[145] http://enigmail.mozdev.org/home/index.php
[146] http://www.gnupg.org/
[147] http://www.claws-mail.org/
[148] http://sylpheed.sraoss.jp/en/
[149] http://www.washington.edu/alpine/
[150] https://www.google.com/accounts/NewAccount?service=mail
[151] http://security.ngoinabox.org/en/riseup_createaccount
[152] http://security.ngoinabox.org/en/node/1451#3.3
[153] https://security.ngoinabox.org/fr/thunderbird_securite
[154] https://security.ngoinabox.org/avast_principale
[155] https://security.ngoinabox.org/comodo_principale
[156] https://security.ngoinabox.org/spybot_principale
[157] https://security.ngoinabox.org/fr/firefox_autres
[158] https://security.ngoinabox.org/fr/thunderbird_utiliserenigmail
[159] http://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique
[160] http://www.mozilla.com/firefox
[161] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/firefox/Firefox3.6.3fr.exe
[162] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/firefox/noscript-1.9.9.80.xpi
[163] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/firefox/formfox-1.6.3-fx.xpi
[164] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/firefox/petname_tool-1.6-fx.xpi
[165] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/firefox/firegpg.xpi
[166] https://security.ngoinabox.org/firefox_noscript
[167] https://security.ngoinabox.org/firefox_autres
[168] https://security.ngoinabox.org/ccleaner_main
[169] https://addons.mozilla.org/fr/firefox/
[170] http://noscript.net/
[171] http://noscript.net/faq
[172] http://getfiregpg.org/install.html
[173] https://www.torproject.org/
[174] https://security.ngoinabox.org/sites/security.ngoinabox.org/security/files/tor/vidalia-bundle-0.2.1.26-0.2.9.exe
[175] https://security.ngoinabox.org/chapter-8
[176] http://www.google.com
[177] http://mail.google.com
[178] https://mail.google.com
[179] https://security.ngoinabox.org/tor_resolutiondesproblemes
[180] https://security.ngoinabox.org/firefox_principale
[181] https://check.torproject.org/
[182] https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ
[183] https://bridges.torproject.org/
[184] http://www.youtube.com
[185] http://www.dailymotion.com/
[186] http://hub.witness.org/
[187] https://www.torproject.org/torbutton/
[188] https://www.torproject.org/torbutton/faq.html.en
[189] http://www.torproject.org/torbrowser/index.html.fr/
[190] https://check.torproject.org
[191] https://security.ngoinabox.org/tor_reseau
[192] https://security.ngoinabox.org/tor_principale